مجموعه کتاب‌های مرکز عملیات امنیت

روز دوم

نگاهی به معماری و مانیتورینگ امنیتی شبکه

برگرفته از مفاهیم شارژ SANS

مؤلفان:

سید سعید حسینی

مریم مکاریان خراسانی

NAGHOOS PUBLICATION

۱۳۹۸

سرشناسه	: حسینی، سید سعید ،۱۳۶۰-
عنوان و نام پدیدآور	: نگاهی به معماری ومانیتورینگ امنیت شبکه برگرفته از مفاهیم شرکت SANS / مولفان سید سعید حسینی، مریم مکاریان خراسانی
مشخصات نشر	: تهران: ناقوس، ۱۳۹۸.
مشخصات ظاهری	: ۱۹۰ص.: مصور.
فروست	: مجموعه کتابهای مرکز عملیات امنیت؛ روز دوم .
شابک	: 978-600-473-215-4
وضعیت فهرست نویسی	: فیپا
موضوع	: کامپیوترها – ایمنی اطلاعات
موضوع	: Computer security-- Management
موضوع	: شبکه های کامپیوتری— تدابیر ایمنی
موضوع	: Computer networks—Security measures
موضوع	: حفاظت داده ها
موضوع	: Data protection
شناسه افزوده	: مکاریان خراسانی ، مریم و ۱۳۷۱-
رده بندی کنگره	: QA ۷۶/۹
رده بندی دیویی	: ۰۰۵/۸
شمارهٔ کتابشناسی ملی	: ۵۸۲۴۸۵۵

انتشارات ناقوس

برای خرید Online به آدرس زیر مراجعه کنید:

www.naghoos.com.ir

NAGHOOS PUBLICATION

نام کتاب	: مرکز عملیات امنیت (نگاهی به معماری ومانیتورینگ امنیت شبکه برگرفته از مفاهیم شرکت SANS)
ناشر	: انتشارات ناقوس
مولفین	: سید سعید حسینی، مریم مکاریان خراسانی
ناظر چاپ	: یاسمن تجلی محدث
چاپ اول	: ۱۳۹۸
تیراژ	: ۱۰۰۰جلد
چاپ و صحافی	: برجسته
قیمت	: ۴۰۰۰۰۰ ریال
شابک	: ۹۷۸ -۶۰۰-۴۷۳-۲۱۵-۴
ISBN	: 978-600-473-215-4

انتشارات ناقوس

بلوار کشاورز- خیابان ۱۶آذر- کوچه پارسی- پلاک ۱۰

تلفن و فاکس : ۶۶۴۷۸۹۵۷-۶۶۴۷۸۹۵۸

فهرست مطالب

فصل سوم: فایروال‌های Stateful Inspection

فصل چهارم: فایروال برنامه کاربردی وب

فصل پنجم: NIPSs & NIDSs

فصل ششم: فایروال‌های نسل بعدی

فصل هفتم: دستگاه Detonate بدافزار

فصل هشتم: Forward Proxy

فصل نهم: SIEM/SIM/SEM

فصل دهم: دستگاه‌های ضبط بسته

فصل یازدهم: دستگاه‌های فریب دشمن

فصل دوازدهم: هوش تهدید

فصل سیزدهم: NSM

منابع و مأخذ

مقدمه

تقریبا هر شرکت در حال حاضر حداقل دارای برخی از تجهیزات امنیتی دفاعی سایبری مانند فایروال، پیشگیری از نفوذ، فیلتر ایمیل و آنتی ویروس می‌باشد. اینها اصول درستی هستند، اما آیا این تجهیزات برای محافظت از شرکت شما واقعا کافی هستند؟

در مجموعه کتاب‌های مرکز عملیات امنیت، جنبه‌های مختلفی از امنیت اطلاعاتی را به صورت عمیق بررسی خواهیم کرد. موضوعات اصلی مورد بررسی، موارد زیر خواهند بود:

- معماری امنیتی[1]
- مراکز عملیات امنیت[2]
- نظارت بر امنیت شبکه[3]
- نظارت مستمر امنیتی[4]

سازمان شما با پیچیده سازی مواردی که در این مجموعه کتاب‌ها بررسی می‌شوند، می‌تواند سریعاً به موفقیت دست پیدا کند، اما مدیریت بر امنیت اطلاعات توجه دائمی می طلبد. کتاب روز اول با بررسی وضعیت فعلی امور مربوط به امنیت اطلاعات شروع می شود. سپس به بررسی تهدیدهای محیط فعلی و معماری امنیتی سنتی و مرسوم می پردازد.

معماری فعلی در چه مواردی با موفقیت عمل می کند؟

کدام راه‌حل‌های سنتی و مرسوم نمی‌توانند پاسخگوی چالش‌های فعلی باشند؟

با بررسی پاسخ‌های پرسش‌های بالا به کاستی‌های معماری فعلی پی خواهیم برد و با تغییراتی که برای برطرف کردن آنها الزامی است آشنا خواهیم شد.

یکی از چالش‌هایی که با آن مواجه هستیم تغییرات مداوم چشم انداز[5] تهدیدات است. اگرچه یک معماری امنیتی قوی شبکه وکاربر نهایی[6] در جلوگیری از رخنه[7]، نسبت به راه‌حل‌های استاندارد، موفق‌تر عمل می‌کند، ولی آنها هم شکست می‌خورد. قبل از اینکه سعی کنیم چیزی را بهبود ببخشیم، نیاز داریم که بدانیم چطور آسیب می‌بیند. باید ابتدا نقاط قوت و ضعف معماری‌های سنتی و رایج را بررسی کرده، قابلیت‌های موجود برای مانیتورینگ را تشخیص داده و نقطه هدف مورد نظر سازمان را تعریف کنیم. جنبه دیگر ارزیابی وضع موجود، بررسی محیط موجود برای تشخیص[8] است. نظارت مستمر

---

1. Security Architecture
2. Security Operations Centers
3. Network Security Monitoring (NSM)
4. Continuous Security Monitoring (CSM)
5. landscape
6. End-point
7. Compromise
8. detection

امنیتی یک جزء مورد نیاز برای معماری امنیتی مدرن است و پاسخگویی سریع به تهدیدات پیش نشده بعدی را تسهیل می‌کند.

در روز دوم از مجموعه کتاب‌های مرکز عملیات امنیت، تأکید کلیدی بر معماری امنیت شبکه قابل دفاع[1] است. در بخش اول شاخصه‌های کلیدی[2] یک معماری امنیتی شبکه قابل دفاع تعریف می شود و بعد از تعریف اصول[3] یک معماری امنیت شبکه قابل دفاع، دستگاه‌هایی که می‌توانند این اصول را پیاده سازی کنند مانند روترها و سوئیچ‌ها، فایروال‌ها، سیستم‌های پیشگیری و تشخیص نفوذ[4]، فایروال‌های برنامه‌های تحت وب[5]، سیستم‌های اطلاعات امنیتی و مدیریت رویداد[6] و غیره، معرفی و بررسی می‌شوند.

هدف از این کار ایجاد یک چک لیست از ابزارهای امنیتی نیست که با قرار دادن علامت در کنار هر یک، تصور امن بودن شبکه برایمان ایجاد شود. ممکن است دو سازمان با داشتن دستگاه‌هایی دقیقا شبیه و یکسان در دو سطح کاملا متفاوت امنیتی عمل کنند. نکته کلیدی در تفاوت نحوه انجام تنظیمات، افرادی که این کار را انجام می دهند و کاری که برای این دستگاه‌ها تعریف شده است، می‌باشد. تنظیمات[7]، افراد[8] و رویه‌ها[9] واردی هستند که این دستگاه‌ها را برای یک معماری امنیت شبکه قوی[10] کارآمد می‌کنند.

حتی در معماری امنیت شبکه و کارآمد نهایی[11] با وجود استفاده از حداکثر توانایی‌ها و قابلیت‌ها، رخنه[12] وجود خواهد داشت. یکی از جنبه‌های کلیدی در معماری امنیتی، تشخیص وجود سیستم‌هایی که به آن‌ها رخنه شده و یا تشخیص سوء استفاده از ظرفیت‌های موجود، می‌باشد. فقط تولید داده‌های مربوط به امنیت کافی نیست و ما باید به طور مؤثر و کارآمد از حجم زیاد داده تولید شده، استفاده کنیم. منابع کلیدی داده‌ها، داده‌های همبسته[13]، داده مربوط به هشدارها[14]، داده مربوط به جلسات[15]،

1. Defensible network security architecture.
2. key characteristics
3. Principles
4. IDS/IPS
5. web applications firewall
6. Security information and event management systems (SIEMs)
7. configuration
8. people
9. processes
10. Robust network security architecture.
11. End-point
12. compromise
13. correlated data
14. alert data
15. session data

داده مربوط به بسته‌های شبکه[1]، داده لاگ‌ها[2]، داده مربوط به کاربر نهایی[3]، کاربر و داده‌های مربوطه[4] و مربوطه[4] و فراداده‌ها[5] می‌باشند که در نظارت بر امنیت شبکه[6] مورد استفاده قرار می‌گیرند.

در روز سوم از مجموعه کتاب‌های مرکز عملیات امنیت، بر روی معماری امنیتی کاربر نهایی تمرکز می‌شود. زیرا دشمنان[7] بر روی رخنه[8] به کاربران نهایی از طریق اکسپلویت‌های سمت کاربر، متمرکز شده‌اند. دفاع در برابر این نوع خاص از حملات، با راه‌های ساده‌ای که توسط معماری امنیت شبکه سنتی[9] پیشنهاد می‌شود، بسیار مشکل است.

با افزایش وجود و حضور دستگاه‌های موبایل و دستگاه‌های قابل حمل در محدوده محیط سازمانها، حملات سمت کاربران نیز افزایش یافته است و این دستگاه‌ها نیز از معماری امنیت شبکه مدرن بهره‌ای نمی‌برند.

انجام عملیات pivoting[10] یکی دیگر از جنبه‌های حملات مدرن است که نیاز به داشتن امنیتی قوی در کاربر نهایی را افزایش می‌دهد. بعد از رخنه به یک کاربر نهایی ضعیف، تکنیک رایج دشمنان، pivot کردن و دسترسی به بقیه سازمان است. این حملات این گونه به نظر می‌رسند که توسط دشمنان داخلی انجام شده است در حالی که نفوذگر از سیستم رخنه شده اولیه[11] به عنوان نقطه‌ای برای شروع حمله[12] به شبکه داخلی استفاده می‌کند. پس کاربر نهایی[13] باید بتواند از خود دفاع کند و به شناسایی حملات نیز کمک کند.

بعد از طراحی یک معماری امنیتی قوی[14] و به کارگیری اصول نظارت بر امنیت شبکه[15]، باید اطمینان حاصل کنید وضعیت سیستم‌ها و شبکه‌ها با اصول و قوانین امنیتی دلخواه سازمان شما هماهنگی و سازگاری داشته باشد.

تهدیدها و آسیب‌پذیری‌ها هر روزه افزایش پیدا می‌کنند و تاکتیک‌های جدید به طور مؤثری کارایی و امنیت سازمان شما را دستخوش تغییر می‌کنند. اگر ما از وضعیت آگاهی[16] نداشته باشیم، نمی‌توانیم تصمیمات آگاهانه در مورد اقدامات امنیتی اتخاذ کنیم. در روز چهارم مجموعه کتاب‌های مرکز عملیات

---

1. packet data
2. log data
3. endpoint data
4. user and attribution data
5. Metadata
6. Network Security Monitoring
7. adversaries
8. compromise
9. Traditional Network Security architecture
۱۰. معادل دیجیتالی جهش نظامی (military leapfrogging) یا پرش جزیره‌ای (island hopping) می‌باشد.
11. initially compromised system
12. beachhead
13. End-point
14. robust security architecture
15. network Security Monitoring principles
16. situational awareness

امنیت، نظارت مستمر بر امنیت[1] که امکان بررسی و آگاهی از وضعیت فعلی امنیت سازمان را فراهم می کند، بررسی می شود. اگرچه بررسی و مرور مستمر وضعیت اجزای سیستم های یک سازمان، نسبتا مطلوب و ساده به نظر برسد ولی بدون داشتن یک پروسه و رویه مشخص، اینکار بسیار سنگین و پرزحمت خواهد بود.

اگرچه سازمان ها و شرکتها معمولاً بر طبق زمانبندی به تعمیر و نگهداری سیستم عامل های ویندوز و بررسی و حسابرسی[2] می‌پردازند ولی دشمنان[3] برای انجام حمله و رخنه[4] به سیستم‌ها هیچ زمان‌بندی مشخصی ندارند و منتظر اسکن‌های سه ماهه و یا حسابرسی‌های سالانه[5] سازمان‌ها نمی‌شوند. باید آگاه باشیم که چگونه تغییرات تهدیدها، آسیب‌پذیری‌ها و دارایی‌ها[6] بر روی امنیت سازمان‌ها تأثیر گذارند و این مستلزم ارزیابی مستمر سازمان است. برای دستیابی به ارزیابی مستمر تغییرات حوزه تهدیدها و آسیب‌پذیری‌ها، خودکارسازی[7] نیاز است. در این کتاب از پاورشل[8]، دستورات ساده اسکریپت نویسی در خط فرمان ویندوز و اسکریپت نویسی Bash برای این کار استفاده خواهیم کرد.

1. Continuous Security Monitoring
2. audit
3. adversaries
4. compromise
5. Quarterly scans or annual audits
6. assets
7. automation
8. PowerShell