معماری امنیت شبکه

مرجع حرفه‌ای طراحی شبکه امن

شون کانوری
CCIE® No. 4232

مترجم: **محمد صادق دوستی**
ویراستاران علمی: **احسان ملکیان**
نوید باباخانی

ناشر کتب فنی مهندسی کامپیوتر دانشگاهی
نص

سرشناسه	: کانوری، شون	Convery, Sean
عنوان و پدیدآور	: **معماری امنیت شبکه** /مؤلف شون کانوری؛ [مترجم] محمد صادق دوستی؛ ویراستار علمی احسان ملکیان، نوید باباخانی.	
مشخصات نشر	: تهران: نص، ۱۳۸۶.	
مشخصات ظاهری	: ۵۲۰ص. جدول، مصور	
شابک	: ۶۵۰۰۰ ریال	ISBN: 978-964-410-119-9
وضعیت فهرست‌نویسی	: فیپا.	
یادداشت	: عنوان اصلی. Network security architectures, c2004	
یادداشت	: کتابنامه.	
موضوع	: شبکه‌های کامپیوتری، اقدامات تامینی.	
موضوع	: منطق، راهنمای آموزشی (متوسطه).	
شناسه افزوده	: دوستی، محمدصادق، ۱۳۶۲، مترجم.	
رده‌بندی کنگره	: ۱۳۸۶ ۶م۲۵ک/TK۵۱۰۵/۵۹	
رده‌بندی دیویی	: ۰۰۵/۸	
شماره کتابشناسی ملی	: ۱۱۱۷۲۰۱	

موسسه علمی فرهنگی

معماری امنیت شبکه

مولف : شون کانوری

مترجم : محمد صادق دوستی

ویراستاران علمی : احسان ملکیان

نوید باباخانی

چاپ اول : زمستان ۸۶

شمارگان: ۲۰۰۰

ناشر:«نص»

چاپ و صحافی: سازمان چاپ و انتشارات وزارت فرهنگ و ارشاد اسلامی

طراحی، آماده‌سازی: موسسه علمی فرهنگی «نص»

قیمت : ۶۵۰۰ تومان

تهران: میدان انقلاب، خیابان اردیبهشت، بن بست مبین، شماره ۲۳۷

تلفکس: ۶۶۴۱۲۳۸۵ - ۶۶۹۵۳۸۸۳ - ۶۶۴۶۵۶۷۴ ص.پ. ۸۶۳-۱۳۱۴۵

شابک: ۹-۱۱۹-۴۱۰-۹۶۴-۹۷۸ ISBN: 978-964-410-119-9

تقدیم

تقدیم به پدر و مادرعزیزم

دربارهٔ نویسنده

شـــون کـــانوری (Sean Convery)، CCIE No. 4232[1] از مـــعمارین امـــنیت Cisco Systems VPN و Security Business Unit است. وی بیشتر در فناوریهای نوین تمرکز دارد. اکنون بیش از شش سال از همکاری شون با سیسکو می‌گذرد. شهرت او بیشتر به خاطر پایه‌گذاری Cisco SAFE Blueprint است. در خلال این چند سال، وی با هزاران مشتری سیسکو مشاورهٔ امنیتی داشته و طرحهای امنی را برای شبکه‌های گوناگون در اندازه‌های مختلف ارائه نموده است. شون پیش از ورود به سیسکو، ۱۲ سال در زمینه‌های مختلف IT و امنیت شبکه فعالیت داشته است. وب سایت تخصصی او را می‌توانید در آدرس زیر پیدا کنید:

http://www.seanconvery.com

---

۱. مدرک CCIE معتبرترین مدرک سیسکو است. هر فردی که این مدرک را دریافت کند، با یک شمارهٔ ویژه شناخته می‌شود- مترجم.

پیش‌گفتار

امروزه امنیت شبکه بخش قابل توجهی از بودجهٔ IT سازمانها را به خود اختصاص می‌دهد. ترس از خطر حملات اینترنتی بودجهٔ به مراتب بیشتری را به سازمانها تحمیل می‌کند.

کتابهای سنتی در زمینهٔ امنیت IT دیگر چندان کاربردی نیستند. ترتیب قدیمی «اول محرمانگی، بعد یکپارچگی، بعد دسترسی‌پذیری» کاملاً وارونه شده است. با وجود حملات DDoS، امروزه دسترسی‌پذیری در اولویت نخست قرار دارد. اما چطور می‌توان با حملاتی که از آسیب‌پذیری سیستم سایر افراد – و نه سیستم شما – سوء استفاده می‌کنند دست و پنجه نرم کرد؟

کتابهایی که در زمینهٔ رمزنگاری نوشته شده‌اند چندان مناسب شما نخواهند بود. آنها جزئیات ریاضی و الگوریتمهای رمزنگاری را بیان می‌کنند، حال آنکه شما به مثالهای کاربردی نیاز دارید.

می‌توان امنیت IT را با رشتهٔ پزشکی مقایسه کرد: دیگر دورانی که دانشجویان پزشکی می‌توانستند همه چیز را از یک کتاب فرا بگیرند به سر آمده است. در عوض، آنها باید منابع گوناگونی را مطالعه کنند. به علاوه، آنها باید کتابهای مقدماتی در رابطه با آناتومی و زیست شیمی را نیز بررسی نمایند. از این گذشته، مطالعهٔ کتب طب بالینی که به تشریح چگونگی شیوع بیماری و مقابله با آن می‌پردازد نیز به همان اندازه مهم است.

در زمینهٔ امنیت IT، کتابهای تئوری بسیاری نوشته شده‌اند. ما به «کتب بالینی» امنیت اطلاعات نیاز داریم؛ که بر اساس تجارب واقعی نوشته شده باشند.

به همین دلیل است که خیلی از کتاب شون کانوری خوشم آمد. شون یکی از معماران امنیت سیسکو است، و این مسیریابهای سیسکو هستند که اینترنت را سرپا نگه می‌دارند. بنابراین دید و تجربهٔ او قطعاً شما را یاری خواهد کرد.

امروزه طراحی و پیکربندی شبکه‌ها به گونه‌ای که در مقابل بدشانسی، خطا، و حمله مقاوم باشند چیزی شبیه جادو است. شاید در آینده بتوان فرمولهای دقیقی برای این کار ارائه داد. اما تا آن موقع، کتاب شون راهنمای شما خواهد بود.

راس اندرسون، پروفسور مهندسی امنیت؛
انگلیس، دانشگاه کمبریج
نویسندهٔ کتاب Security Engineering - A Guide to Building Dependable Systems
جولای ۲۰۰۳

مقدمهٔ مؤلف

تفاوت «طراحی امنیت شبکه» و «طراحی شبکهٔ امن» چیست؟

در ابتدا به نظر می‌رسد که داریم با کلمات بازی می‌کنیم. اما در حقیقت تفاوت در طرز نگرش به مسئله است. «طراحی امنیت شبکه» متضمن این معناست که می‌توان امنیت شبکه را مستقلاً طراحی کرد، بدون آنکه توجهی به شبکهٔ اطراف آن داشته باشیم. از طرف دیگر، «طراحی شبکهٔ امن» به معنای به کارگیری اصول طراحی امن در طراحی شبکه است.

هدف این کتاب ارائهٔ روشی اصولی برای طراحی شبکه‌های امن است. برخلاف سایر کتابهای سیسکو، در این کتاب فرض بر استفاده از تجهیزات سیسکو نیست. این کتاب به شما نفوذگری را نخواهد آموخت. و در آن از تئوریها و اصول ریاضی رمزنگاری خبری نیست. تمرکز ما بر مثالهای کاربردی طراحی خواهد بود. همانطور که خواهید دید، طرحهای این کتاب بر ایده‌ای مهم استوارند: «امنیت شبکه یک سیستم است».

سازماندهی مطالب کتاب

این کتاب به چهار بخش تقسیم شده است:

- **بخش ۱** مبانی امنیت شبکه
- **بخش ۲** طراحی شبکه‌های امن
- **بخش ۳** طرحهای شبکهٔ امن
- **بخش ۴** مدیریت شبکه، مطالعات موردی، و جمع‌بندی

بخش ۱ شامل ۴ فصل است، و اجزای سازندهٔ امنیت شبکه را بررسی می‌کند. هر فصل می‌تواند کتابی مستقل باشد؛ اما در اینجا هدف آن است که مطالب خلاصه‌وار بیان شده تا بتوانید در فصلهای دیگر از آنها استفاده کنید. مطالب فصلهای ۳ و ۴ به ویژه در بخش ۳ کتاب کاربرد دارند.

بخش ۲ شامل ۸ فصل است، و در آن انواع فناوریهایی را که طراح شبکه برای ایجاد شبکه‌ای امن نیاز دارد بررسی می‌کنیم.

بخش ۳ شامل ۳ فصل است، و در آن طرحهای امنیتی را در سه بخش از شبکه (مرز، قلمرو، و شبکهٔ کارکنان راه دور)

مرور خواهیم کرد.
بخش ۴ شامل ۳ فصل است، و در آن پس از بررسی چگونگی مدیریت شبکه‌ها، به چند مطالعهٔ موردی می‌پردازیم. فصل پایانی این بخش (و این کتاب) جمع‌بندی مختصری از مطالب است.

مقدمهٔ مترجم

خدا را شاکرم که توانستم ترجمهٔ کتاب دیگری را به پایان برسانم. آماده‌سازی این کتاب بیش از یک سال به طول انجامید، و امیدوارم خوانندهٔ گرامی از مطالعهٔ آن لذت ببرد.

اما چرا این کتاب؟ اگر پیشگفتار و مقدمه مؤلف را خوانده باشید، احتمالاً تا حدودی به پاسخ این پرسش واقف هستید. اما دوست دارم در اینجا بار دیگر بر آن تأکید کنم؛ این بار با نگاهی بر آنچه در دانشگاههای ایران می‌گذرد.

در دانشگاههای ما درسهایی نظیر امنیت شبکه، رمزنگاری مقدماتی و پیشرفته، و نظایر آن ارائه می‌شود، که هریک جذابیتهای خاص خود را دارد و هر سال تعداد زیادی دانشجو در این درسها به صورت اختیاری ثبت نام می‌کنند. در این درسها مبانی تئوری امنیت اطلاعات به دقت بررسی می‌شود. با این وجود جای خالی مباحث عملی و کاربردی در آنها احساس می‌شود.

اینجانب در ترم اخیر (ترم دوم ۸۶) در درس امنیت شبکه دستیار استاد بودم، و سعی کردم مطالب کاربردی این کتاب را در کلاس مطرح کنم، که خوشبختانه با استقبال خوب دانشجویان مواجه شد.

البته علاوه بر دانشجویان، این کتاب برای سایر قشرهای جامعه که در زمینهٔ امنیت شبکه (و حتی طراحی شبکه) فعالیت می‌کنند نیز مفید خواهد بود.

در ترجمهٔ کتاب سعی کردم که تا حد ممکن از واژه‌های فارسی به جای معادل لاتین استفاده کنم، و گاه به معادل‌سازی هم روی آوردم. اگر در فهم واژه یا کوته‌نوشتی دچار اشکال شدید، واژه‌نامهٔ انتهای کتاب (که شامل بیش از ۸۰۰ مدخل است) راهنمای شما خواهد بود.

ترجمه این کتاب توسط استاد بزرگوار جناب آقای مهندس احسان ملکیان و مهندس نوید باباخانی مورد بازخوانی و ویرایش قرار گرفت، که از ایشان صمیمانه سپاس‌گزارم.

در پایان لازم می‌دانم از مدیر انتشارات نص، جناب آقای زارع، و مسئول بخش فنی، جناب آقای رمضانی، که از هیچ کوششی برای ارتقای سطح این کتاب دریغ نکردند تشکر کنم.

بخش ۱

مبانی امنیت شبکه

فصل ۱ بدیهیات امنیت شبکه

فصل ۲ چرخه عمر سیاستها و اقدامات امنیتی

فصل ۳ تهدیدات امنیت شبکه

فصل ٤ فناوریهای امنیت شبکه

فصل ۱

بدیهیات امنیت شبکه

این فصل شامل مطالب زیر است:

- امنیت شبکه یک سیستم است
- نیازهای کاری باید در اولویت قرار بگیرند
- طراحی شبکهٔ امن مستقل از طراحی شبکه نیست
- همه چیز هدف است
- همه چیز سلاح است
- سعی کنید کارها از نظر عملیاتی ساده باشند
- امنیت شبکهٔ خوب قابل پیش‌بینی است
- امنیت از طریق پنهان‌کاری بدست نمی‌آید
- محرمانگی و امنیت با هم تفاوت دارند

یکی از عواملی که در طراحی شبکه‌های امن به شما کمک می‌کند، درک قوانین پایه است. من این قوانین را «بدیهیات» می‌نامم. بنا به تعریف واژه نامهٔ Meriam-Webster، بدیهیات «اصولی هستند که بدلیل ماهیت آشکار خود توسط عموم مردم پذیرفته شده‌اند». وقتی در این کتاب سخن از این بدیهیات به میان می‌آورم، منظور من اصول، ملاحظات، یا توصیه‌های طراحی است که به اندازهٔ کافی جامع هستند که بتوان آنها را به تمام طرحهای شبکه‌های امن اعمال کرد. اگر چه «ماهیت آشکار» آنها تا حدودی قابل بحث است، اما سعی کرده‌ام به قدر کافی استدلال کنم تا چنین ادعایی پذیرفتنی باشد.

تفاوت بدیهیات با اصول آن است که اصول محدودتر از بدیهیات هستند، و اغلب تنها به یک فناوری یا بخش محدودی از شبکه اعمال می‌شوند. مثلاً، عبارت زیر یک اصل طراحی است:

> **سیستم‌های تشخیص نفوذ** *(IDS:Intrusion-Detection System)* **باید تا حد ممکن در نزدیکی میزبانی که قرار است از آن محافظت شود نصب گردند.**

علت آن است که این «اصل» تنها به فناوری IDS محدود است.

بحث این کتاب به دو دلیل با بررسی بدیهیات آغاز می‌شود: اول آنکه آنها در مورد همهٔ آنچه در ادامهٔ کتاب می‌خوانید

صادق هستند، و می‌توانید این بدیهیات را در ذهن داشته باشید و به طرحهای امنیتی اعمال کنید. دوم آنکه اگر این بدیهیات در فصل اول ذکر نمی‌شدند، هر جا به آنها نیاز داشتم باید آنها را تکرار می‌کردم، که باعث می‌شد حجم این کتاب سه برابر شود! فهم صحیح این بدیهیات به شما در فهم طرحهای شبکه‌های امن کمک می‌کند.

امنیت شبکه یک سیستم است

امنیت شبکه یک سیستم است. نمی‌توان آن را معادل حفاظ (firewall) ، IDS ، (Virtual Private Network) ، VPN ، یا AAA (Authentication, Authorization, Accounting) دانست. امنیت چیزی نیست که بتوانید از سیسکو یا سایر شرکتها خریداری کنید. البته محصولات امنیتی جای خود را در این سیستم دارند، اما امنیت شبکه فراتر از این محصولات است. امنیت با یک «سیاست امنیتی» شروع می‌شود؛ و سپس دو شاخه می‌شود: افرادی که باید این سیاستها را رعایت کنند، و افرادی که باید بر اجرای آن نظارت داشته باشند. سرانجامِ کار، اِعمال تغییراتی در زیرساختهای شبکه است.

به عنوان مثال حملات کرمهای شبکه را که در سال ۲۰۰۱ شدت یافت در نظر بگیرید. کرمی نظیر Code Red در ۲۴ ساعت اول بیش از ۳۴۰,۰۰۰ میزبان را آلوده کرد *(http://www.caida.org)*. اگرچه کرمها پدیدهٔ جدیدی نبودند و بسیاری از این میزبانها به وسیلهٔ حفاظ محافظت می‌شدند، اما از آنجا که اغلب این حفاظها به بررسی دقیق بسته‌ها نمی‌پرداختند، و چون حمله روی پورت ۸۰کار می‌کرد به آن اجازهٔ عبور می‌دادند، Code Red توانست از حفاظها عبور کند. حتی حفاظهایی که بسته‌ها را به دقت بررسی می‌کردند هم از این حمله مصون نبودند، چون حملهٔ Code Red جدید و ناشناخته بود. با عبور این کرم از حفاظها، هیچ چیز مانع از تهاجم Code Red به شبکهٔ داخلی نمی‌شد. یک **سیستم** قادر بود با Code Red مقابله کند، اما حفاظ به تنهایی از هیچ شانسی برخوردار نبود.

حال ببینیم مفهوم سیستم در رابطه با امنیت شبکه چیست. به طور کلی **سیستم امنیت شبکه** به صورت زیر تعریف می‌شود:

> **مجموعه‌ای از ابزارها و فناوریهای شبکه به همراه روشهای پذیرفته شده[1] که در همکاری با یکدیگر امنیت دارایی‌های اطلاعاتی را تأمین می‌کنند.**

مهمترین واژه در این تعریف، «**همکاری**» است. اگر چه هر یک از ابزارها می‌توانند به تنهایی یا در کنار هم بخشی از امنیت را تأمین کنند، اما برای رسیدن به سطح مطلوبی از امنیت به همکاری ابزارها، فناوریها، و رفتارهای صحیح (رعایت توصیه‌ها و..). نیاز داریم. برخی از متخصصین امنیت اطلاعات این مفهوم را «دفاع چندلایه» (defense-in-depth) می‌نامند. یکی از راههای بررسی کیفیت امنیت یک سیستم آن است که تعیین کنید در برابر هر حمله، چند لایهٔ دفاعی وجود دارد. چنین تحلیلی در سطوح ابتدایی طراحی شبکه‌های امن مفید است، اما کمی که پیش رفتید و تمام لایه‌های دفاعی را چیدید، باید تعیین کنید که طرح بدست آمده در برابر چند نوع حمله مقاوم است.

به عنوان مثال اجازه دهید کرم پورت ۸۰ را بار دیگر بررسی کنیم. چه عناصری از سیستم امنیتی می‌توانند حمله به سرور وب توسط یک کرم مبتنی بر HTTP را خنثی کنند؟ لیست زیر عناصر را –که در فصل ۴ بررسی شده‌اند– ذکر می‌کند:

---

۱. best practices- در اصطلاح به مجموعه‌ای از روشها و توصیه‌ها اطلاق می‌شود که تجربه نشان داده است که در صورت رعایت آنها، به بهترین نتایج دست می‌یابیم. این روشها و توصیه‌ها مورد پذیرش اهل فن قرارگرفته است– مترجم.

- حفاظی که به درستی پیکربندی شده باشد می‌تواند مانع از آسیب رساندن یک سرور وب تسخیر شده (compromised) به سایر بخشهای شبکه گردد.
- LANهای مجازی خصوصی (Private Virtual LAN) (PVLANها؛ نه VLANهای عادی؛ برای اطلاعات بیشتر فصل ۶ را ببینید) می‌توانند مانع از آلوده شدن سیستمهای شبکه توسط سرور وب شوند.
- NIDS (Network IDS) می‌تواند تلاش برای آلوده‌سازی سرور وب را کشف و خنثی کند.
- HIDS (Host IDS) می‌تواند همان عملکرد NIDS را داشته باشد، اما مزیت HIDS آن است که به میزبان نزدیک‌تر است؛ که عموماً به معنای در اختیار داشتن اطلاعات بیشتر از حمله است.
- ضدویروسها می‌توانند کرمها و سایر کدهای مضر را تشخیص دهند؛ مشروط بر آنکه پایگاه دادهٔ علائم (Signature database) آنها به روز شده باشد.
- در نهایت، اگر چه بررسی وظایف مسئول سیستم (sysadmin: System administrator) موضوع این کتاب نیست، اما تبعیت مسئولین سیستم از روشهای پذیرفته شده نظیر به روز رسانی به موقع، پویش منظم آسیب‌پذیریهای شبکه، محبوس کردن (lockdown) سیستم عامل، و پیاده‌سازی توصیه‌های امنیتی سرور وب می‌تواند تفاوت شگرفی در امنیت شبکه ایجاد کند.

همه عناصر فوق در همکاری با یکدیگر مانع از وقوع حمله می‌شوند. اگرچه هر عنصر نمی‌تواند به طور قطعی کرمهای مبتنی بر HTTP را متوقف کند، اما با یک بررسی سادهٔ احتمالی مشخص می‌شود که وقتی از چند لایهٔ دفاعی استفاده می‌کنید، امکان خنثی شدن حمله افزایش می‌یابد.

ارزش اصلی سیستم امنیتی وقتی مشخص می‌شود که بتواند در برابر حملات ناشناخته مقاومت کند. مثلاً یکی از وقایع امنیتی زیر را در نظر بگیرید:

- کرم Moris (نخستین کرم) در سال ۱۹۸۸؛
- ابزارهای اختفا و جعل IP در دههٔ ۱۹۹۰ (اطلاعات بیشتر در فصل ۳ داده شده است)؛
- حملات DDoS در سال ۲۰۰۰؛
- کرمهای HTTP در سال ۲۰۰۱؛
- SQL Slammer و MS Blaster در سال ۲۰۰۳.

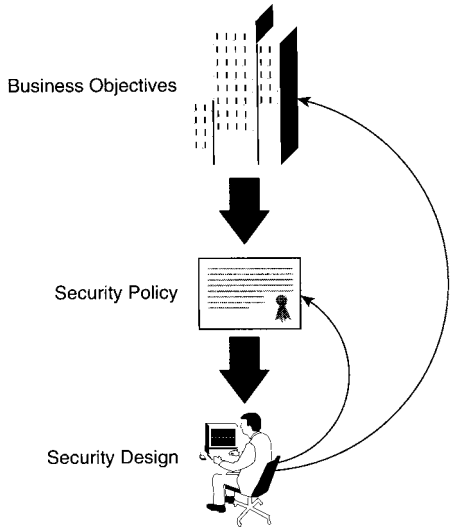
این حملات به ما چیزهای بسیاری آموختند. تنها از طریق این «آموزش دردناک» است که کاستی‌های امنیتی خودی نشان می‌دهند. اگرچه هیچ راهی برای اجتناب از این نوع آموزش وجود ندارد، اما می‌توان با طراحی سیستم امنیتی به گونه‌ای که با گسترهٔ وسیعی از حملات مقابله کند، مشکلات را به حداقل رساند. در حقیقت یکی از معیارهای موفقیت یک سیستم امنیتی، میزان تغییراتی است که باید در صورت کشف حملات جدید به آن اعمال شود.

امنیت شبکه یک **سیستم** است. اگر پس از خواندن این کتاب همهٔ آن را فراموش کنید، من نویسندهٔ بسیار بدی بوده‌ام. اما اگر چند چیز را به یاد بسپارید، امیدوارم این جمله یکی از آنها باشد.

نیازهای کاری باید در اولویت قرار بگیرند

برای اعمال هر تغییر جدید در سیستم امنیتی، سه عامل را باید مدنظر قرار دهید. این عوامل که در شکل ۱-۱ نشان داده شده‌اند – عبارتند از اهداف کاری، سیاست امنیتی، و طرح امنیتی. این شکل مفصلاً در فصل ۲ توضیح داده شده است.

شکل ۱-۱
اولویتهای کاری



آنچه این اصل می‌گوید آن است که اگر بین نیازهای کاری و مسائل امنیتی تناقضی وجود داشت، کدام یک در اولویت قرار می‌گیرد. پاسخ ساده است: نیازهای کاری باید در اولویت قرار بگیرند. خوب، مسئله این است: اگر نیازهای کاری را در اولویت قرار دهیم، چه بر سر امنیت سیستم می‌آید؟ اصلاً در آن صورت چه نیازی به متخصصین امنیتی داریم؟

در اینجا دو شگرد وجود دارد که مسئله را حل می‌کند:

۱. رابطهٔ بین اهداف کاری، سیاست امنیتی، و طرح امنیتی نوعی «همزیستی» است. اگر چه روند کار از بالا به پایین است، اما باید فلشهایی از پایین به بالا هم کشیده شود (شکل ۱-۱). وظیفهٔ طراح امنیتی آن است که مطمئن شود ملاحظات امنیتی در طرح کاری گنجانده شده‌اند.

۲. در روشهای طراحی امنیتی موفق، پیش‌بینی‌هایی برای اعمال تغییرات در آینده گنجانده شده است. به این ترتیب هر بار که نیازهای کاری تغییر می‌کند، نیازی نیست که طراحان امنیتی را فرا بخوانید تا سیستم امنیتی را از نو طراحی کنند. یکی از بهترین روشها، به کارگیری طراحی پیمانه‌ای (modular) است؛ که طرح را به بخشهای مجزای تقسیم می‌کند. در صورت نیاز به تغییر لازم نیست همهٔ بخشها تغییر کند. تمرکز اکثر فصلهای این کتاب بر روی طراحی پیمانه‌ای است.

طراحی شبکهٔ امن مستقل از طراحی شبکه نیست

در گذشته (و حتی این روزها) بارها پیش آمده که یکی از مشتریان به من گفته است: «ما کار طراحی شبکه را به پایان رسانده‌ایم، و اکنون وقت آن است که به امنیت فکر کنیم. قطعاً به یک حفاظ نیاز داریم، و چیزهایی هم دربارهٔ IDS شنیده‌ایم».

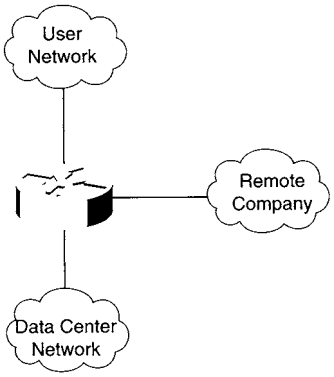
طراحی به این روش که در آن «امنیت» به شبکه «اضافه» می‌شود - باعث کاهش کارآیی شبکه شده و مزاحمتهایی را برای کارمندان IT و تیم عملیاتی شبکه به بار می‌آورد. اگرچه امنیت از دیدگاه طراحی شبکه «مفت» بدست نمی‌آید، اما اگر آن را از ابتدا در طرحهایتان لحاظ کنید می‌توانید به یک طرح متوازن دست یابید. به این ترتیب هم

امنیت شبکه و هم قابلیت اطمینان و گسترش‌پذیری آن بهبود می‌یابد.

اجازه دهید یک مثال ساده را بررسی کنیم. فرض کنید می‌خواهید بین یک مرکز داده، گروهی از کاربران، و یک شرکت راه دور که می‌خواهد به مرکز دادهٔ شما وصل شود ارتباط برقرار نمایید. اگر از امنیت صرفنظر کنید، طرح شما مشابه شکل ۱-۲ خواهد بود.

شکل ۱-۲

طرح بدون امنیت



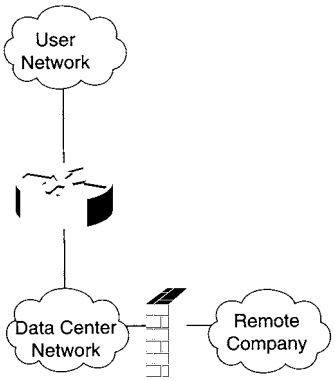
در اینجا ناگهان نمایندهٔ تیم امنیت اطلاعات (INFOSEC: Information Security) سر می‌رسد و می‌گوید: «وای! چه کار می‌کنید؟! چرا شرکت راه دور اجازهٔ دسترسی مستقیم به داده‌های سازمان را دارد؟ ما اینجا به امنیت نیاز داریم!» شما تصمیم می‌گیرید که یک حفاظ نرم‌افزاری را به همراه مجموعه‌ای از ACLها به مسیریاب اضافه کنید تا بتوانید بر جریان اطلاعات بین مرکز داده و شرکت راه دور نظارت داشته باشید. حال که مسیریاب وظیفهٔ حفاظ را هم بر عهده گرفته است، کارآیی آن کاهش می‌یابد. این تنزل کارآیی فقط بین شرکت راه دور و مرکز داده نیست، بلکه کاربران شبکه هم آن را احساس می‌کنند. به این ترتیب امنیت نه تنها بهبودی به همراه نداشته، بلکه بر شبکه تأثیر منفی گذاشته است. حتی اگر از حفاظهای سخت‌افزاری در کنار مسیریاب استفاده کنید، مشکلات ناشی از پیچیدگی پیکربندی دو ابزار را نمی‌توان دست‌کم گرفت.

حال به عقب برگردید و طراحی را از نو و با توجه به نیازمندیهای امنیتی انجام دهید. نتیجه چیزی شبیه شکل ۱-۳ خواهد بود.

در شکل ۱-۳ حفاظی بین مرکز داده و شرکت راه دور نصب شده است که کنترل بیشتری را با کاهش کارآیی

شکل ۱-۳

طرح با امنیت



کمتری دربر دارد؛ راه‌اندازی و نگهداری آن ساده‌تر است؛ و از همه مهمتر، تأثیر سوئی بر ارتباط کاربران با مرکز داده ندارد.

اگر چه این مثال خیلی ساده بود، امیدوارم منظور مرا درک کرده باشید: همیشه سعی کنید امنیت را از ابتدای طراحی در نظر بگیرید. متأسفانه اگر به شما شبکه‌ای بدهند و بخواهند که امنیت آن را بهبود دهید، کار به این سادگی نخواهد بود. در این موارد سعی کنید طرح را به بخشهای کاری کوچکتری تقسیم کنید، و امنیت هر بخش را مستقلاً بهبود دهید. کار را با بخشی شروع کنید که کمترین امنیت را داراست. از طراحی مجدد نهراسید؛ چون کاری که برمبنای طرح بدی استوار شود در آینده شما را با مشکل مواجه می‌کند.

همه چیز هدف است

به عنوان طراحی شبکه‌های امن، یکی از نخستین چیزهایی که باید در نظر بگیرید وابستگی اجزای شبکه به یکدیگر است. یک مهاجم می‌تواند هر یک از این اجزا را به عنوان هدف انتخاب کند و با استفاده از این وابستگی‌ها به هدف نهایی خود برسد.

به عنوان مثال فرض کنید مهاجم قصد دارد سایت وب شما را پایین بیاورد. لیست زیر گزینه‌های پیش روی مهاجم را نشان می‌دهد:

- یک ضعف امنیتی در کاربردها یا سیستم عاملِ سیستم شما پیدا کند، از آن بهره بگیرد تا به اختیارات root دسترسی داشته باشد، سپس به راحتی سرور را پایین بیاورد یا محتوای آن را تغییر دهد.
- جریانی از ترافیک منع خدمت (DOS: Denial of Service) را روانهٔ سرور وب شما کند تا منابع آن مصرف شوند و سرور قدرت پاسخگویی را از دست بدهد.
- با پی‌ریزی یک حملهٔ DDOS، تمام پهنای باند شما را مصرف کند تا کاربران مشروع نتوانند به سرور وب شما دسترسی داشته باشند.
- آن قدر بسته‌های پوچ به سمت مسیریاب یا حفاظ بفرستد که این ابزارها نتوانند بسته‌های مشروع را پردازش کنند.
- سرور DNS شما یا ISP شما را تسخیر کند و رکورد نام سرور وب شما را به یک سرور جعلی تغییر دهد.
- سرور دیگری را در همان زیرشبکهٔ سرور وب شما تسخیر کند و حملهٔ جعل ARP ای را اجرا نماید که یا مانع دسترسی به سرور وب شود و یا با پی‌ریزی یک حملهٔ مرد میانی (MITM: Man In The Middle) محتوا را پیش از ارسال به مقصد تغییر دهد.
- سوییچ اترنتی را که دسترس اینترنتِ سرور وب را فراهم می‌کند تسخیر کرده و پورت مربوطه را غیرفعال نماید.
- اطلاعات مسیردهی ISP شما را تغییر دهد تا درخواستهایی را که به زیرشبکهٔ IP شما فرستاده می‌شوند به جای دیگری هدایت کند.

این لیست تنها به موارد فوق محدود نمی‌شود. در این مثال، مهاجم برای اجرای حمله چندین «هدف» را می‌توانست انتخاب کند، از جمله:

- امنیت کد کاربردها و سیستم عامل
- مقاومت کاربردها و سیستم عامل در برابر DoS
- پهنای باند اینترنت

- مسیریابها یا سایر ابزارهای لایهٔ ۳ (L3)
- هدایت DNS
- مجموعه پروتکل TCP/IP
- ابزارهای لایه ۲ (L2)
- پروتکلهای مسیریابی

لیستی مشابه این را می‌توان برای حمله به هر ابزاری (و نه فقط سرورهای وب) نوشت. به خاطر داشته باشید: همه چیز هدف است.

بسیاری از سازمانها فقط به امنیت سرورهای عمومی (public) خود توجه می‌کنند، و از امنیت سایر ابزارها غافلند. آنها توجه نمی‌کنند که ریسک تسخیر شدن یک سرور عمومی خیلی کمتر از ریسک تسخیر شدن یک سرور e-mail داخلی و لو رفتن طرحهای تجاری سازمان است. شما، به عنوان معمار امنیت، باید روشی را پیشنهاد کنید که از همهٔ سیستمهای شبکه محافظت شود؛ این در حالی است که مهاجم کافیست که تنها یک سیستم پیدا کند که شما به درستی محافظت نکرده‌اید. همان طور که در فصل ۲ خواهید دید، یک سیاست امنیتی خوب به شما کمک می‌کند که بفهمید در مورد چه چیزهایی، و به چه میزان، باید نگران بود.

همه چیز سلاح است

یکی از مهمترین دلایلی که همه چیز هدف محسوب می‌شود آن است که از هر چیز می‌توان به عنوان سلاح استفاده کرد، و مهاجم سعی می‌کند که تا می‌تواند سلاح بدست آورد تا بتواند به هدف بعدی حمله کند. مثلاً فرض کنید مهاجم یک سرور DHCP را تسخیر کرده است. هدف بعدی می‌تواند یکی از موارد زیر باشد:

- مهاجم می‌تواند پس از منقضی کردن تمام آدرسهای IP اجاره داده شده توسط سرور DHCP، این سرویس را متوقف کند تا هر سیستمی که بر مبنای آدرسهای پویا کار می‌کند، دیگر نتواند به شبکه وصل شود.
- مهاجم می‌تواند از سرور DHCP استفاده کند تا حمله‌ای را پی‌ریزی نماید که در آن از اعتمادی که سایر سیستمها به سرور DHCP دارند سوءاستفاده شود تا مهاجم به سیستمهای بیشتری دسترسی پیدا کند.
- مهاجم می‌تواند پیکربندی DHCP را به گونه‌ای تغییر دهد که آدرسهای سرور DNS و درگاه پیش فرضی که در اختیار کلاینت قرار می‌گیرد، جعلی باشند. این آدرسهای جعلی برای کلاینت معتبر به نظر می‌رسند، و باعث می‌شوند کلاینت درخواستهای DNS و ترافیک خارج از شبکه (off-net) را به ماشین مهاجم بفرستد؛ که مقدمه‌ای است بر حملات شنود و MITM.

به جز در حملهٔ اول، مهاجم از سرور DHCP به عنوان سلاحی برای پیشبرد حمله استفاده کرده است. توجه داشته باشید که مهاجم لازم نیست که حتماً از سیستمهای موجود به عنوان سلاح استفاده کند؛ بلکه ممکن است سلاحهای مورد نیازش را خود وارد شبکه کند. با این مفهوم که به «ابزارهای نفوذی» (rogue) مشهور است در فصلهای آتی آشنا می‌شوید.

سعی کنید کارها از نظر عملیاتی ساده باشند

طراحی شبکه‌های امن باید تا حد ممکن ساده باشد؛ به گونه‌ای که تیم عملیاتی شبکه در نگهداری آن با مشکل مواجه نشوند. اگر شبکه از نظر عملیاتی ساده باشد، برایتان به خوبی کار خواهد کرد؛ در غیر این صورت شما باید برای آن

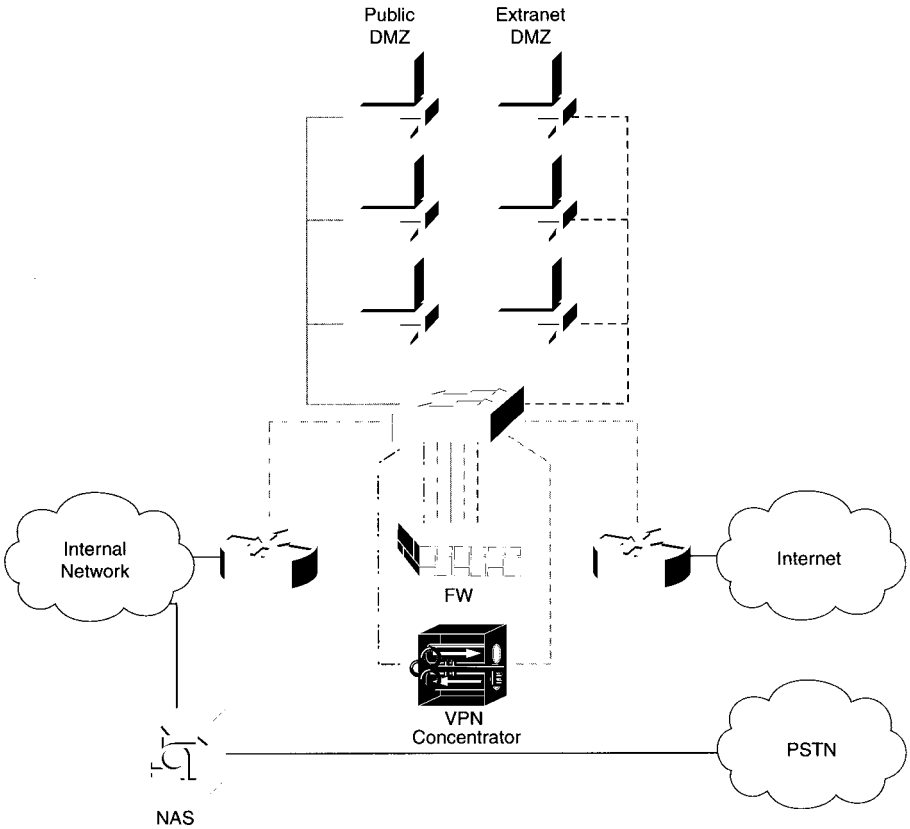
کار کنید!

برخی از معیارهای اندازه‌گیری سادگی عبارتند از:

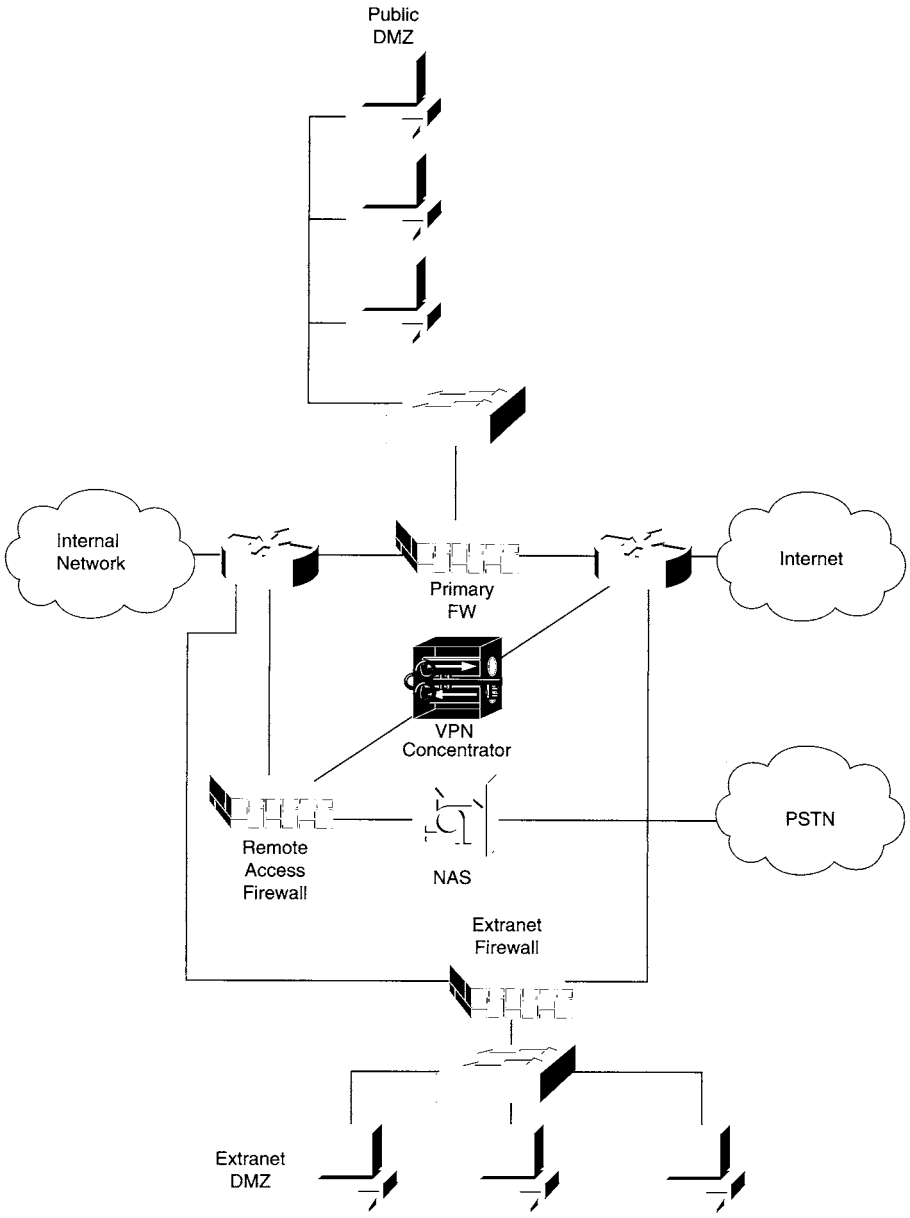
- چند مهندس INFOSEC لازم دارید تا از شبکه نگهداری کنند؟
- در شرایطی که حمله رخ می‌دهد، و اپراتورهای امنیت تحت فشارند، امکان اشتباه چقدر است؟
- وقتی حمله به پایان رسید و سرگرم بررسی جزئیات آن شدید، چه مقدار از فایلهای log را باید بررسی کنید تا به نتیجه برسید؟
- اگر خواستید شواهد قانونی را تقدیم دادگاه کنید، یافتن اطلاعات مرتبط چه مقدار طول می‌کشد؟

با وجود این نباید در مسئلهٔ سادگی خیلی افراط کرد. مثلاً، سادگی عملیاتی الزاماً معادل سادگی همبندی (topology) نیست. بارها شنیده‌ام که طراحان، سادگی همبندی را با عبارتی نظیر «زیبایی» توصیف می‌کنند. متأسفانه باید بگویم که زیبایی در اغلب موارد با کاربردپذیری در تناقض است. اگر نتوانید به موقع و به آسانی به تهدیداتی که متوجه شبکه شماست پاسخ دهید، زیبایی ناشی از همبندی ساده به چه درد می‌خورد؟

بگذارید مثالی بزنم. مرز (edge) اینترنت بسیاری از شبکه‌های سنتی مشابه شکل ۱-۴ است. اگرچه همبندی این طرح ساده است، اما این سادگی مشکلات زیادی را به همراه دارد. یکی از این مشکلات امکان خطای انسانی است، که ناشی از پیچیدگی عملیاتی این طرح است. خطای انسانی ریشهٔ بسیاری از مشکلات پیکربندی است؛ به



شکل ۱-٤ طرح مرز اینترنت سنتی



شکل ۱-۵ طرحی با سادگی عملیاتی

ویژه هنگامی که مسئولین شبکه مجبور می‌شوند ساعت ۲ صبح از خواب بلند شوند و به رفع اشکال از شبکه بپردازند. اگر چه طرح شکل ۱-۴ ساده به نظر می‌رسد، اما پیکربندی حفاظ متصل به سوییچ به غایت مشکل و پیچیده است. در صورتی که اپراتور کوچکترین اشتباه را در پیکربندی این حفاظ مرتکب شود، امنیت کل سیستم به خطر خواهد افتاد.

برای حل این معضل می‌توان از طرح شکل ۱-۵ استفاده کرد، که همبندی آن در نگاه اول خیلی پیچیده‌تر است.

فهم همبندی شکل ۱-۵ ساده‌تر است، و کمتر پیش می‌آید که کسی در پیکربندی آن دچار اشتباه شود. اگر چه این طرح از ابزارهای بیشتری استفاده می‌کند و به «زیبایی» طرح شکل ۱-۴ نیست، اما مسیرهای ارتباطی و بخشهای امن و ناامن آن به وضوح مشخصند. در این طرح بهبود یافته، اتصال اینترنت توسط یک حفاظ و اتصال VPN از طریق حفاظی دیگر کنترل می‌شود. به علاوه به جای استفاده از یک سوییچ L2 با چند VLAN، از سوییچ‌های L2 مجزایی استفاده شده است. به این ترتیب تعریف قوانین دسترسی و تغییر در پیکربندیها ساده‌تر انجام خواهد شد.

امنیت شبکهٔ خوب قابل پیش‌بینی است

شما باید نقاط قوت و ضعف شبکه‌تان را به درستی بشناسید. خریداری کورکورانهٔ آخرین فناوریها و نصب آنها در شبکه به امید آنکه بالاخره یکی موفق خواهد شد جلوی حمله را بگیرد کار درستی نیست. به یاد داشته باشید که امنیت توسط زنجیره‌ای از ابزارها، فناوریها، و روشهای پذیرفته شده تأمین می‌شود. مقاومت این زنجیره تنها در حد ضعیف‌ترین حلقهٔ آن است. بنابراین نباید به صرف اینکه از «آخرین» یا «بهترین» فناوریها و ابزار استفاده می‌کنید تصور کنید که امنیت شبکه برقرار شده است. طراحی صحیح و پیکربندی درست سبب می‌شود که در صورتی که با تهدید جدی روبه رو شدید بتوانید سریعاً آن را دفع کنید، یا حداقل بدانید که کجای سیستم در برابر این تهدید آسیب‌پذیر است و فوراً آن را ترمیم کنید. به طور خلاصه، باید بتوانید سیستم امنیتی قابل پیش‌بینی داشته باشید. برای این منظور باید:

۱. بتوانید مشکلات و رخدادهایی را که سیستم ممکن است تجربه کند (نظیر حملات) درک کنید.
۲. نحوهٔ ساخت سیستمی را که با حملات مقابله می‌کند در نظر بگیرید.
۳. شرایطی را که ممکن است سیستم را به خرابی بکشاند در نظر گرفته و لایه‌های دفاعی منظمی را برای مقابله آن ایجاد کنید.

این مسائل باید هنگام طراحی در نظر گرفته شوند، وگرنه احتمال اینکه سیستم غیرقابل پیش‌بینی باشد افزایش می‌یابد. این موضوع به امنیت شبکه محدود نمی‌شود؛ بلکه در سایر رشته‌ها نیز کاربرد دارد: مقاومت بدنهٔ اتومبیلها و ایمنی آنها در برخورد با موانع تست می‌شود؛ طرح ساختمانها در شرایط زمین‌لرزه مورد بررسی قرار می‌گیرد؛ و نظایر آن.

در اینجا چند مثال آورده شده تا موضوع روشنتر شود:

- اگر حفاظی که مسئول محافظت از یک سرور وب بوده به اشتباه پیکربندی شود، و به جای اینکه فقط به ترافیک روی پورت مشخصی اجازهٔ عبور دهد همهٔ پورتها را باز کند، چه اتفاقی می‌افتد؟ در یک روش طراحی پیش‌بینی‌پذیر، چنین احتمالی در نظر گرفته می‌شود، و طراح نمودار درختی تبعات آن را ارائه می‌کند. در این نمودار ابتدا بیان می‌شود که چه بر سر سرور می‌آید، و سپس تبعات بعدی با فرض تسخیر شدن سرور بیان می‌گردند.
- اگر در یک IPsec VPN با دسترسی‌پذیری بالا (HA: High Availability) میان سایت مرکزی و شعبه‌های آن، خرابی رخ دهد، چه اتفاقی می‌افتد؟ در یک طرح پیش‌بینی‌پذیر از یک ابزار پشتیبانی در سایت مرکزی استفاده می‌شود، حال آنکه در طرحی که پیش‌بینی‌پذیر نیست، امکان استفاده از چنین ابزاری تنها پس از وقوع خرابی در نظر گرفته می‌شود.

طراحان شبکه همواره موضوع پیش‌بینی‌پذیری را در نظر می‌گیرند. مسائلی نظیر بار شبکه، زمان خرابی، زمان پاسخ، و نظایر آن همواره در کلاسهای آموزشی تعلیم داده می‌شود. متأسفانه طراحان امنیتی آن قدر که باید به این

مسئله توجه نمی‌کنند. گاه تبعات این مسئله فراتر از حد انتظار است. بهترین راهکار آن است که طراحی امنیت و شبکه به طور همزمان صورت پذیرد؛ موضوعی که الگوی این کتاب بر مبنای آن استوار است.

امنیت از طریق پنهان‌کاری بدست نمی‌آید

این جمله را بارها شنیده‌اید: «امنیتی که مبتنی بر پنهان‌کاری (obscurity) باشد، امنیت نیست». متأسفانه خیلی‌ها منظور این جمله را به درستی درک نمی‌کنند. اجازه دهید با دو مثال موضوع را روشن کنم:

- پول کاغذی مبنای بسیاری از مبادلات روزمره است، و نگرانی‌هایی در مورد جعل اسکناس وجود دارد. اگر چه کشورها می‌توانند اطلاعات مربوط به کاغذ و جوهر اسکناس را مخفی نگاه دارند، اما چنین کاری نمی‌کنند. در عوض، روشهای دیگری برای مقابله با جعل به‌کار گرفته شده‌اند. این روشها عبارتند از استفاده از عکس شخصیتها در پس زمینه، نخ اسکناس، جوهر قابل دید زیر نور ماورای بنفش، و نظایر آن. در این مورد، برای نیل به امنیت از پنهانکاری استفاده نشده است. البته انتظار نداشته باشید که بانک مرکزی جزئیات چاپ اسکناس را منتشر کند!
- یک مهاجم باهوش می‌تواند نوع و نسخهٔ حفاظهای مورد استفاده در یک شبکه را بدست آورد (به کمک ابزاری نظیر Nmap، که از آدرس *http://www.insecure.org* قابل دریافت است). بنابراین امنیت شبکه شما نباید وابسته به مخفی نگه داشتن این اطلاعات باشد؛ بلکه باید مطمئن شوید که حفاظ وظیفهٔ کنترل دسترسی را به درستی انجام می‌دهد. با این وجود، لازم نیست اطلاعات حفاظ خود را در اختیار عموم قرار دهید!

موضوع مثال قبل، پنهان کاری نوع و نسخه حفاظ بود. مثال بعد ارزش پنهان کردن وجود یک فناوری امنیتی در شبکه را نشان می‌دهد:

- در چند سال اخیر بسیاری تلاش کرده‌اند تا بفهمند که آیا از NIDS در شبکه استفاده شده است یا نه، و اگر پاسخ مثبت بود، مکان و پیکربندی آن را استخراج کنند. هدف این مهاجمین آن است که بدانند دستشان تا چه حد باز است و سعی کنند از ضعفهای موجود در پیکربندی نهایت استفاده را ببرند. برای مقابله با این افراد باید پیکربندی و محل NIDS را محرمانه نگه دارید. در اینجا شما از «امنیت از راه پنهان کاری» تبعیت نمی‌کنید؛ بلکه عقل سلیم حکم می‌کند که این اطلاعات را مخفی نگه دارید.

در آدرس زیر مقاله‌ای در رابطه با فریب NIDS وجود دارد:

http://secinf.net/info/ids/idspaper/idspaper.html

- گاه از NAT (Network Address Translation) به عنوان روشی برای ایمنی بیشتر یاد می‌شود. در حقیقت، تنها کاری که NAT انجام می‌دهد پنهان کردن آدرسهای لایهٔ ۳ است. حتی اگر NAT هم استفاده شود، باز هم به کنترل دسترسی نیاز دارید. یک حفاظ دارای حالت کامل می‌تواند این کنترل را در لایه ۳ و ۴ انجام دهد، و علاوه بر آن قادر است وظایف پیچیده‌تری را نیز بر عهده بگیرد. NAT نمی‌تواند هیچ یک از این کارها را انجام دهد، حتی اگر از ترجمهٔ چند به یک استفاده کنید. در این رابطه مفصلاً در فصل ۶ بحث شده است.

همچنین توجه کنید که NAT (و تا حدودی حفاظ) می‌تواند امنیت شبکه را کاهش دهد، چون کاربران سعی خواهند کرد ترافیک را روی پورتهای مجاز تونل کنند؛ که دسته‌بندی ترافیک را مشکل می‌کند. البته مزایای حفاظ بر چنین مشکلی می‌چربد، اما هنگام طراحی سیاستهای کنترل دسترسی باید به آن توجه داشته باشید.

امیدوارم با این مثالها منظور مرا درک کرده باشید. البته مفهوم این گفته‌ها آن نیست که هرگز نباید از سازوکارهای پنهان کاری بهره جست؛ بلکه امنیت سیستم نباید متکی بر پنهان‌کاری باشد. اگر پنهان کردن عناصری از طرح امنیتی برای مسئولین شبکه مشکلی به همراه ندارد، به کارگیری پنهان‌کاری معقول است. در مقابل، اگر با پنهان‌کاری بار مسئولین شبکه را زیاد می‌کنید، اغلب بهتر است که از آن صرفنظر شود.

به عنوان مثال، مخفی کردن اعلان (banner) ورود ابزارها (که اغلب شامل نوع و نسخهٔ نرم‌افزار آن است) دردسر زیادی به همراه ندارد، و بهتر است انجام شود. در عوض، تغییر پورت پیش‌فرض پروتکلهای معروف (مثل تغییر پورت پروتکل SMTP از ۲۵ به ۲۵۲۵) سبب می‌شود که تمام کاربردها تغییر داده شوند تا از پورت جدید استفاده کنند؛ و این یعنی سخت کردن کار مسئولین شبکه، و افزایش تماسها با مرکز پشتیبانی شبکه شما.

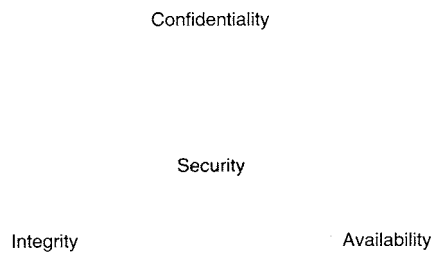
محرمانگی و امنیت با هم تفاوت دارند

محرمانگی و امنیت با هم تفاوت دارند. در اینجا تعریفی از هر یک را مشاهده می‌کنید: **محرمانگی** حفاظت از اطلاعات است به گونه‌ای که افراد غیرمجاز نتوانند آن را بخوانند. **امنیت** حفاظت از سیستمها، منابع و اطلاعات است تا از دسترسی ناخواسته و غیرمجاز و سوءاستفاده در امان باشند.

تفاوت آشکار است: محرمانگی زیرمجموعه‌ای از امنیت است؛ چون امنیت تنها به محافظت از اطلاعات محدود نمی‌شود. در یک تعریف نسبتاً ساده شده می‌توان امنیت را مبتنی بر سه عنصر دانست که به سه‌گانه CIA مشهورند (شکل ۱-۶):

- محرمانگی (Confidentiality)
- یکپارچگی (Integrity)
- دسترس‌پذیری (Availability)

شکل ۱-۶
سه‌گانهٔ CIA



وقتی به طراحی شبکه‌های امن می‌پردازید باید دیدی فراتر از محرمانگی اطلاعات داشته باشید، و مطمئن شوید که از کل شبکه به درستی استفاده می‌شود؛ حتی اگر تمام ارتباطات بین عناصر شبکه محرمانه باشند.

خلاصه

امیدوارم که آنچه در این فصل به عنوان بدیهیات امنیت شبکه ارائه شد، واقعاً واضح و بدیهی بوده و شما آنها را به راحتی پذیرفته باشید. البته اگر بیشتر اطلاعات این فصل برایتان تازگی داشت، جای نگرانی نیست؛ اکنون شما دانشی بنیادین در اختیار دارید که بر مبنای آن می‌توانید مفاهیم فصلهای آتی را بنا کنید.

مرجع

- *Tippett, P. "Defense-In-Breadth." Information Security Magazine (February 2002). http://www.infosecuritymag.com/2002/feb/columns_executive.shtml*