

禪

اصول طراحی امنیت شبکه

چگونه امنیت یک شبکه کامپیوتری را تامین کنیم؟

پیادهسازی یک مکانیزم امنیتی گسترشپذیر و کارآمد در یک شبکه، مستلزم بهکارگیری یک طراحی مناسب و منطبق بر نتایج به دست آمده از تحلیل ریسکها و خطمشیهای حاکمیتی است. مکانیزمهای امنیتی شبکه اولین سد دفاعی برای محافظت از منابع سیستمی در برابر تهدیدات خارجی همچون کدها و اسکریپتهای مخرب و هکرها است. مکانیزمهای امنیتی مهم برای دفاع در برابر تهدیدات سایبری دیوارهای آتش، سامانههای شناسایی و پیشگیری از نفوذ، شبکههای خصوصی مجازی و سامانههای بررسی محتوای فایلها (ضدویروسها، ضدبدافزارها، ضدهرزنامهها و مسدودکنندگان آدرسهای اینترنتی هستند .) ترکیب راهحلهای سختافزاری و نرمافزاری مانع از آن میشود تا هکرها بتوانند به سادگی به سیستمعامل، بانکهای اطلاعاتی و نسخههای پشتیبان از اطلاعات دسترسی پیدا کرده و اطلاعات را ویرایش، سرقت یا پاک کنند .

برای آنکه بتوان یک سیستم امنیتی گسترشپذیر و ایمن را برای یک شبکه متوسط یا بزرگ طراحی کرد، لازم است ریسکهای سازمان به درستی شناسایی شده و خطمشیهای امنیتی متناسب با اهداف سازمان تدوین شوند .

خطمشیها و اصول امنیتی

بهطور کلی، خطمشیها و اصول امنیتی که اجازه میدهند از سامانههای فناوریاطلاعات و شبکه یک سازمان محافظت کرد شامل موارد زیر میشوند :

دفاع یکپارچه و همه جانبه

همانگونه که در شکل زیر مشاهده میکنید برای محافظت از منابع فناوریاطلاعات به لایههای امنیتی مختلفی نیاز دارید . در دکترین امنیتی دفاع همه جانبه شامل رعایت موارد زیر میشود :

- E-mail antivirus
- E-mail anti-spam
- User authentication
- HTTP antivirus
- Server IPS
- User authentication
- Server IPS
- Server antivirus
- User authentication
E-mail server
Web, DNS servers
SQL servers
Intranet server
File server
Internet
User workstations
- Network firewall
- Network IPS
- IPSec VPN gateway
- Web application firewall
- Network antivirus
- URL filtering
- Network firewall
- Network IPS
- User authentication
- Personal firewall
- Antivirus scanner
- User authentication

[illegible]

[illegible]

[illegible]

[illegible]

آنها باشد .

ضعیفترین عنصر موجود در زنجیره امنیت

سطح ایمنی سامانههای فناوریاطلاعات در برابر تهدیدات به ضعیفترین عنصر موجود در این حلقه بستگی دارد . کارشناسان امنیتی میدانند که همواره باید به اصل SPOF سرنام Single Point of Failure توجه خاصی داشته باشند. اصل فوق در ارتباط با دسترسپذیری سرویسهای شبکه است. مطابق با این اصل تمامی لینکها، تجیهزات شبکه و امنیت، سرورهای موجود در شبکه که نقش پلی برای برقراری ارتباط میان کاربران و منابع مهم را ایفا میکنند باید در پیکربندیهای مربوط به افزونگی مورد توجه قرار گیرند . در زمان پیادهسازی مکانیزم امنیتی شبکه لازم است تا قواعد مهمی همچون تفکیک وظایف و گردش شغلی مورد توجه قرار گیرد . این اصول با هدف محدود کردن توانایی کارمندان در نادیده گرفتن دستورالعملها یا نقض خطمشیهای امنیتی به کار گرفته میشوند . تفکیک وظایف بیانگر این موضوع است که وظایف و عملکردهای مهم در هر بخش باید توسط دو یا چند کارمند محدود انجام شود . گردش شغلی نیز اعلام میدارد کارمندان نباید در یک سازمان برای مدت زمان مدیدی در یک پست باقی بمانند و لازم است بهطور متناوب جایگاه شغلی آنها تغییر کند .

تقسیمبندی حوزههای امنیتی

دیوارهای آتش اصلیترین مکانیزم دفاعی در برابر تهدیدات هستند که جریان ترافیک شبکه را زیر نظر گفته و محدودیتهایی در ارتباط با ارسال یا دریافت دادهها ایجاد میکنند . دیوارهای آتش زمانی که همراه با سامانههای تشخیص نفوذ و فهرستهای کنترل دسترسی در سوییچها و روترها استفاده شوند یک لایه امنیتی قدرتمند به وجود میآورند . اگر دیوارهای آتش به شکل درستی استقرار پیدا کرده و پیکربندی شوند، شبکههای بزرگ به زیرشبکههای کوچکتر تقسیم شوند و تقسیمبندی حوزههای امنیتی متناسب با قواعد استاندارد انجام شود، زیرساختهای ارتباطی شبکه توسط یک معماری امنیتی قدرتمند محافظت خواهند شد. در دکترین طراحی امنیت شبکه، اصل تقسیمبندی قواعد زیر را شامل میشود :

منابع سامانههای فناوریاطلاعات با سطوح مختلف حساسیت باید در حوزههای امنیتی مختلفی قرار گیرند .

تجهیزات و سامانههای ارائهدهنده خدمات به شبکههای خارجی همچون اینترنت باید در حوزههای مختلفی همچون De-Militarized Zone قرار گیرند تا اگر حملهای انجام شود، سامانهها و تجهیزات داخلی شبکه آسیب نبینند .

منابع کلید و مهم فناوریاطلاعات باید در حوزههای امنیتی ویژهای قرار گیرند .

تجهیزات و سامانههایی که قابلیت اطمینان پایینی دارند همچون سرورهای دسترسی از راه دور و نقاط دسترسی بیسیم در شبکه باید در حوزههای امنیتی خاصی استقرار یابند .

منابع سیستمی مختلف فناوریاطلاعات باید در حوزههای امنیتی جداگانه از یکدیگر قرار گیرند تا در صورت بروز حمله آسیبدیدگی به حداقل برسد .

ایستگاههای کاری کارمندان باید در حوزههای امنیتی خاصی مستقر شوند .

سامانههای مدیریت امنیت و شبکه باید در حوزههای امنیتی خاص قرار گیرند .

پیشگیری از نفوذ

تجهیزاتی همچون سامانههای پیشگیری از نفوذ، دیوارآتش تحت برنامه (WAF) و.... مسئولیت شناسایی و مسدودکردن نفوذها و حملاتی را عهدهدار هستند که توسط هکرها و برنامههای مخرب پیادهسازی میشوند . سامانههای فوق باید در مسیر شبکه داخلی و شبکه خارجی و همچنین منابع حساسی که احتمال نفوذ به آنها وجود دارد نصب شوند. با توجه به اینکه ممکن است هکرها حملات مبتنی بر نشستهای رمزگذاری شده را پیادهسازی کنند باید این مسئله توسط سامانههای IPS مورد توجه قرار گیرد . در حالت معمول، سامانه

IPS نمیتواند نشستهای رمزگذاری شده را بررسی کند، به همین دلیل اگر نشستها قبل از رسیدن به IPS رمزگشایی شوند، این امکان وجود دارد تا مانع شکلگیری برخی از حملات شد . در یک مکانیزم امنیتی خوب شبکههای داخلی به شکل مستقیم به اینترنت دسترسی ندارند، زیرا هکرها ممکن است از طریق یک حمله فیشینگ تروجانی برای یک ایستگاه کاری ارسال کنند و سامانه کاربر را قربانی کنند . در چنین شرایطی اگر شبکه داخلی در پشت یک دیوارآتش پنهان شده باشد، هکر قادر نخواهد بود به شبکه داخلی دسترسی پیدا کند . شکل زیر نحوه پیادهسازی چنین مکانیزمی را نشان میدهد . در شکل زیر سرویسرهای اینترنتی برای کاربران تنها از طریق ایمیل سازمانی و سرورهای مبتنی بر HTTP Proxy در دسترس هستند.

Mail server
Web Cache (HTTP Proxy)
SMTP, IMAP/POP3
Intrusion Prevention, Anti-Malware
HTTP, HTTPS
HTTP, HTTPS
SMTP
Internet
Trojan
Firewall
User workstations

در تحلیل ریسکها و طراحی امنیت، همواره تاکید بر ارزشمندترین منابع فناوریاطلاعات همچون سامانههای ارائهدهنده خدمات یا پشتیبان است . با این حال، نباید از ایمنسازی منابع و تجهیزات دیگر غافل شد. برخی از کارشناسان امنیتی از راهکار Island Hopping برای مقابله با حملات سایبری استفاده میکنند . Island Hopping روی این اصل مهم تاکید دارد که کسب مجوز دسترسی غیرمجاز به حوزههای محافظت شده از طریق نقاط ضعیفی انجام میشود که برای سازمان حائز اهمیت نیستند. به همین دلیل از این نقاط به عنوان نقطه شروعی برای نفوذ و دسترسی به منابع ارزشمندتر و محافظت شده یک سازمان استفاده میشوند . شناسایی و پاسخگویی به حوادث و نقصهای امنیتی باید در کوتاهترین زمان ممکن انجام شود و در زمان تدوین برنامه امنیتی باید به موارد یاد شده اشاره شده باشد . بهطور مثال، باید شرایطی همچون یک حمله مبتنی بر آسیبپذیری روز صفر در نظر گرفته شود . حملهای که بر مبنای آن سامانه پیشگیری از نفوذ قادر به شناسایی آن نیست و در نتیجه یک هکر به راحتی موفق میشود به زیرساخت ارتباطی یک شبکه نفوذ کند . به همین دلیل باید یک چنین شرایطی خاصی در برنامه امنیتی موردبررسی قرار گرفته و تهمیدات لازم در نظر گرفته شده باشد . همچنین فراموش نکنید مسئولان دپارتمان امنیت باید گزارشها و هشدارها را بهطور مرتب بررسی کرده، ترافیک و فعالیتهای روزمره در شبکه را زیر نظر گرفته و با اصول مدیریت شبکههای محلی مجازی آشنا باشند .

نویسنده :
حمیدرضا_تائبی
دسته بندی:
فناوری شبکه
امنیت
تاریخ انتشار :
07:35 - 17/12/1398
برچسب:

□□□□□
https://www.shabakeh-mag.com/networking-technology/16645/%DA%86%DA%AF%D9%88%D9:□□□□
%86%D9%87-%D8%A7%D9%85%D9%86%DB%8C%D8%AA-%DB%8C%DA%A9-
%D8%B4%D8%A8%DA%A9%D9%87-
%DA%A9%D8%A7%D9%85%D9%BE%DB%8C%D9%88%D8%AA%D8%B1%DB%8C-
%D8%B1%D8%A7-%D8%AA%D8%A7%D9%85%DB%8C%D9%86-
%DA%A9%D9%86%DB%8C%D9%85%D8%9F