**مرجعی بر امنیت**

**مبتنی بر**

# CompTIA **Security+**

تقدیم به

یاور و یاری رسان همیشگی ام

تقدیم به همسر عزیزم

بنام ایزد منان

# مرجعی بر امنیت

## مبتنی بر

# CompTIA Security+

مهندس مجید داوری دولت آبادی

عضو گروه امنیت GrayHat Hackers

Security Information Assets

انتشارات پندار پارس

سرشناسه : داوری دولت‌آبادی، مجید، ۱۳۵۹ -
عنوان و نام پدیدآور : مرجعی بر امنیت مبتنی بر + CompTIA Security/ مجید داوری‌دولت‌آبادی.
مشخصات نشر : تهران: پندار پارس: سخنوران: مانلی، ۱۳۸۹.
مشخصات ظاهری : ۵۴۴ ص.: مصور ، نمودار .
شابک : ۱۳۵۰۰۰ ریال:۹۷۸-۹٦٤-۲۹۸۹-۵۸-٤
وضعیت فهرست نویسی : فیپا
موضوع : شبکه‌های کامپیوتری -- اقدامات تامینی
موضوع : کامپیوترها -- ایمنی اطلاعات
رده بندی کنگره : ۱۳۸۹ ۴م۲د/۵۱۰۵/۵۹TK
رده بندی دیویی : ۸/۰۰۵
شماره کتابشناسی ملی : ۵۴۶۲۷۲۲

*انتشارات پندارپارس*

**www.pendarepars.com دفتر فروش:** انقلاب، ابتدای کارگرجنوبی، کوی رشتچی، شماره ١٤، واحد ١٦
**info@pendarepars.com** تلفن: ٦٦٥٧٢٣٣٥ - تلفکس: ٦٦٩٢٦٥٧٨ همراه: ۰۹۱۲۲٤٥۲۳٤۸

**نام کتاب** : **مرجعی بر امنیت، مبتنی بر + CompTIA Security**
**ناشر** : **انتشارات پندار پارس ناشر همکار: سخنوران، مانلی**
**ترجمه و تالیف** : **مهندس مجید داوری دولت آبادی**
**چاپ اول** : **اسفند ۸۹**
**شمارگان** : **۱۰۰۰ نسخه**
**طرح جلد** : **محمد اسماعیلی هدی**
**لیتوگرافی، چاپ، صحافی** : **ترام‌سنج، صالحان، روشنک**
**قیمت** : **۱۳۵۰۰ تومان** **شابک : ٤-۵۸-۲۹۸۹-۹٦٤-۹۷۸**

# فهرست


**فصل اول مفاهیم اساسی امنیت ..... ۱**

مقدمه ..... ۲

مفهوم امنیت اطلاعات ..... ۲

امن‌سازی محیط‌های فیزیکی ..... ۳

بررسی امنیت عملی ..... ۸

طرز عملکرد سیاست‌ها و مدیریت‌ها ..... ۹

ساختارهای کلی سیاست امنیتی ..... ۱۸

اهداف امنیت اطلاعات ..... ۱۸

درک مفهوم فرآیندهای امنیتی ..... ۱۹

تفکیک و بررسی توپولوژی‌های امنیتی ..... ٤۸

توپولوژی‌های امنیتی پیرامون ..... ٤۸

معماری لایه‌ای در توپولوژی‌های امنیتی ..... ۵۰

ناحیه‌های امنیتی ..... ۵۳

مکانیزم شبکه‌های محلی مجازی ( VLANs ) ..... ٦۰

امنیت در VLANها ..... ٦۵

پیاده‌سازی مکانیزم NAT ..... ٦٦

شبکه VPN چیست؟ ..... ٦۸

مدیریت خطر ..... ٦۹

ارزیابی خطر ..... ۷۰

محاسبه فرمولی خطر ..... ۷۰

شناسایی و ارزیابی دارایی‌ها ..... ۷۱

ارزیابی تهدید ..... ۷۲

شناسایی تهدید ..... ۷۲

مراجع این فصل ..... ۷۳

سؤالات چهار گزینه‌ای این فصل ..... ۷۳

پاسخ سؤالات چهار گزینه‌ای این فصل ..... ۷٦

**فصل دوم شناسایی خطرات و حملات شبکه ..... ۷۹**

مکانیزم بازرسی و پیگیری ..... ۸۰

استراتژی انواع حملات برعلیه شبکه ..... ۸۱

اصول کلی پروتکل TCP/IP ..... ۹۲

پروتکل‌های لایهٔ شبکه TCP/IP ..... ۱۰۱
بررسی ارتباطات لایهٔ انتقال ..... ۱۰۷
دست‌تکانی سه مرحله‌ای TCP ..... ۱۱۰
مفهوم پویش کردن ..... ۱۱۱
پویشگرها ..... ۱۱۲
پویش کردن ARP ..... ۱۱۴
پویش پروتکل ICMP ..... ۱۱۵
مروری بر کدهای مُخرب ..... ۱۱۷
مراجع این فصل ..... ۱۲۱
سؤالات چهار گزینه‌ای این فصل ..... ۱۲۲
پاسخ سؤالات چهار گزینه‌ای این فصل ..... ۱۲۵
**فصل سوم زیرساخت‌ها و ارتباطات ..... ۱۲۷**
مقدمه ..... ۱۲۸
مفهوم زیرساخت‌های امنیتی ..... ۱۲۹
امن‌سازی تجهیزات زیربنایی شبکه‌های مختلف ..... ۱۳۵
نظارت، کنترل و شناسایی شبکه‌ها ..... ۱۷۱
مفهوم تجهیزات قابل حمل ..... ۱۷۹
مفهوم دسترسی از راه دور ..... ۱۹۰
امن سازی ارتباطات اینترنت ..... ۲۰۱
مروری بر برخی پروتکل‌های شبکه ..... ۲۳۰
اساس کابل‌ها، سیم‌ها و ارتباطات ..... ۲۳۶
بررسی تجهیزات ذخیره‌سازی قابل حمل ..... ۲۴۶
مراجع این فصل ..... ۲۶۰
سؤالات چهار گزینه‌ای این فصل ..... ۲۶۱
پاسخ سؤالات چهار گزینه‌ای این فصل ..... ۲۶۴
**فصل چهارم سیستم‌های نظارت و تشخیص نفوذ فعال ..... ۲۶۷**
مفاهیم تشخیص، پیشگیری و جلوگیری از نفوذ ..... ۲۶۹
سیستم‌های تشخیص نفوذ (IDS) ..... ۲۷۱
اساس سیستم تشخیص نفوذ ..... ۲۷۶
انواع سیستم‌های تشخیص نفوذ ..... ۲۷۸
سیستم‌های تشخیص نفوذ توزیع شده ..... ۲۸۶
تیم پاسخگویی به حوادث امنیتی ..... ۲۸۷

عملکرد سیستم‌های بی‌سیم ..... ۲۹۵
پروتکل‌های شبکه بی‌سیم ..... ۳۰۳
پروتکل WEP ..... ۳۰۷
مکانیزم‌های تشخیص در سیستم‌های تشخیص نفوذ و احتمال خطا ..... ۳۰۸
بررسی ویژگی‌های پیغام‌های فوری ..... ۳۱۰
شناسایی آسیب‌پذیری‌های پیغام‌های فوری ( IM ) ..... ۳۱۳
مراجع این فصل ..... ۳۱٤
سؤالات چهار گزینه‌ای این فصل ..... ۳۱٤
پاسخ سؤالات چهار گزینه‌ای این فصل ..... ۳۱۷
**فصل پنجم پیاده‌سازی و نگه‌داری شبکه‌های امن ..... ۳۱۹**
ارتقاء امنیت در سطح شبکه ..... ۳۲۰
پیاده‌سازی مدل‌های امنیتی پایه‌ای ..... ۳۲۵
طبقه‌بندی و ایمن‌سازی اطلاعات ..... ۳۲۸
امن‌سازی سیستم‌های سخت‌افزاری و نرم‌افزاری ..... ۳۲۹
ایجاد معماری امن در سیستم‌عامل ..... ۳۳۸
سخت‌گیری‌های امنیتی درخصوص سیستم‌های‌عامل محلی و شبکه ای ..... ۳۳۹
سخت‌گیری امنیتی در خصوص برنامه‌های کاربردی سرورها ..... ۳٤٤
عملکرد انبار داده ..... ۳۵۸
سرویس‌های دایرکتوری ..... ۳۵۹
پروتکل LDAP ..... ۳٦۱
مزایای امنیت و آسیب‌پذیری‌های امنیتی LDAP ..... ۳٦۳
مراجع این فصل ..... ۳٦٤
سؤالات چهار گزینه‌ای این فصل ..... ۳٦٤
پاسخ سؤالات چهار گزینه‌ای این فصل ..... ۳٦۷
**فصل ششم امن‌سازی شبکه و محیط‌های پیرامون ..... ۳۶۹**
مفهوم امنیت فیزیکی ..... ۳۷۰
مروری بر لایه امنیت فیزیکی ..... ۳۷۷
امنیت فیزیکی در کامپیوترهای قابل‌حمل ..... ۳۸۰
موقعیت‌یابی فیزیکی جهت استقرار تجهیزات شبکه ..... ۳۸۱
مهندسی امنیت در سازمان‌ها ..... ۳۸۲
چرخه حیات یک سیستم از دیدگاه امنیتی ..... ۳۸٤
طرح بازیابی پس از بحران و تداوم کسب و کار ..... ۳۸٦

مدیریت متمرکز و غیر متمرکز ..... ۳۸۸
استراتژی حفاظت از اطلاعات..... ۳۸۹
توسعه سیاست‌ها، استانداردها و دستورالعمل‌ها..... ۳۹۵
مستندسازی معماری سیستم‌ها..... ۴۰۱
مدیریت خطرات امنیتی ..... ۴۰۲
اطلاعات کنترل‌های دسترسی..... ۴۰۷
مراجع این فصل..... ۴۰۹
سؤالات چهار گزینه‌ای این فصل..... ۴۰۹
پاسخ سؤالات چهار گزینه‌ای این فصل..... ۴۱۲
**فصل هفتم استانداردها، روش‌ها و اصول اولیه رمزنگاری ..... ۴۱۵**
مروری بر مفاهیم رمزنگاری ..... ۴۱۶
پنهان‌نگاری و تفاوت آن با رمزنگاری..... ۴۲۰
مفهوم پروتکل رمزنگاری..... ۴۲۰
بررسی الگوریتم‌های رمزنگاری ..... ۴۲۹
مقایسه رمزنگاری کلید متقارن و کلید نامتقارن..... ۴۵۰
بهره گیری از سیستم‌های رمزنگاری..... ۴۵۰
بهره گیری از زیربنای کلید عمومی ( PKI )..... ۴۵۱
منظور از CA..... ۴۵۲
مدل‌های مختلف پیکربندی CA ..... ۴۵۴
پیاده‌سازی گواهینامه‌ها..... ۴۵۹
مفهوم امضاهای دیجیتالی..... ۴۶۱
مفاهیم پایه‌ای درخصوص کلید ..... ۴۶۳
مدیریت متمرکز و غیرمتمرکز کلید..... ۴۶۸
مدیریت کلید توسط روش‌های کلید عمومی..... ۴۶۸
الگوریتم‌های تبادل کلید ..... ۴۶۹
منظور از خلاصه پیام‌ها ..... ۴۷۱
مراجع این فصل..... ۴۷۴
سؤالات چهار گزینه‌ای این فصل..... ۴۷۵
پاسخ سؤالات چهار گزینه‌ای این فصل..... ۴۷۸
**فصل هشتم روال‌ها و سیاست‌های امنیتی ..... ۴۸۱**
عوامل اساسی و تأثیرگذار در ایجاد مشکلات امنیتی..... ۴۸۲
مدیریت آسیب‌پذیری..... ۴۸۷

مدیریت کاربران با بهره‌گیری از گروه‌ها ..... ٤٨٩
تهدیدات برپایه منابع انسانی ..... ٤٨٩
عوامل اساسی در مهندسی سیستم‌های امنیتی..... ٤٩٩
مرکز عملیات امنیت شبکه..... ٤٩٩
مراجع این فصل..... ٥٠٣
سؤالات چهار گزینه‌ای این فصل..... ٥٠٣
پاسخ سؤالات چهار گزینه‌ای این فصل..... ٥٠٦
**فصل نهم  مدیریت و اجرای امنیت ..... ٥٠٩**
پروتکل تبادل اطلاعات تونل..... ٥١٠
اساس تونل‌ها در مکانیزم VPN ..... ٥١١
اصول پروتکل IPSec..... ٥١٢
پیادهسازی VPNهای مبتنی بر IP..... ٥١٦
دسته‌بندی‌های مختلف سرویس VPN..... ٥١٨
عملکرد پروتکل SSL ..... ٥١٩
امن‌سازی رسانه‌های انتقال ..... ٥٢١
امنیت در شبکه‌های بی‌سیم..... ٥٢٢
مراجع این فصل..... ٥٢٣
سؤالات چهار گزینه‌ای این فصل..... ٥٢٣
پاسخ سؤالات چهار گزینه‌ای این فصل..... ٥٢٦

## سخنی با خوانندگان

امنیت یک موضوع پیچیده است که از نظر تاریخی تنها توسط افراد با تجربه و آنهایی که آموزش کافی دیده‌اند مورد توجه قرار می‌گیرد. با این‌حال، همچنان که افراد بیشتری به شبکه‌های کامپیوتری متصل می‌شوند، تعداد افرادی که بایستی اصول امنیت را در دنیای شبکه شده بدانند، نیز افزایش می‌یابد. مهمترین وظیفه یک شبکه کامپیوتری فراهم‌سازی امکان برقراری ارتباط میان گره‌های آن در تمام زمان‌ها و شرایط گوناگون است، به‌صورتی‌که برخی از محققین، امنیت در یک شبکه را معادل استحکام و عدم بُروز اختلال در آن می‌دانند. امینت در یک شبکه علاوه بر امنیت کاربردی به معنی خصوصی بودن ارتباطات نیز می‌باشد. شبکه‌ای که درست عمل کند و مورد حمله ویروس‌ها و عوامل خارجی قرار نگیرد، اما درعوض تبادل اطلاعات میان دو نفر در آن توسط دیگران شُنود شود، ایمن نیست.

امن‌سازی اطلاعات هنری است که پیاده‌سازی آن تنها توسط کارشناسان و متخصصان این حرفه صورت می‌گیرد. این متخصصان علوم مختلف علم امنیت و امنیت اطلاعات و ارتباطات را براساس دوره‌ها و استانداردهای ساخت‌یافته فرا گرفته‌اند که و بر همین اساس نیز آن‌را پیاده‌سازی و اجرا می‌کنند. این دوره‌ها برای یک مدیر بسیار مفید و سودمند است و دانش آن درحین کار عملی به کمک آنها می‌آید. درحال حاضر دوره‌های مختلفی در سطح شاخه امنیت اطلاعات و ارتباطات در دنیای فناوری اطلاعات وجود دارد که هرکدام به قسمتی خاص از این علم می‌پردازند. دوره‌هایی چون Security+، CEH، CISSP، CISM، CISA، CPTP، SCNP، CNSA و CHFI از این جمله هستند. پیش‌نیاز تمامی این دوره‌های امنیتی دوره پایه‌ای Security+ است که به بررسی اصول پایه‌ای علم امنیت اطلاعات و ارتباطات می‌پردازد.

اینجانب به عنوان عضو کوچکی از خانواده بزرگ امنیت و شبکه درصدد گردآوری و تألیف کتابی مرجع به منظور افزایش آگاهی متخصصین، دانشجویان و مدیران شبکه در زمینه امنیت اطلاعات، مدیریت امنیت اطلاعات، شبکه‌های کامپیوتری و دوره پایه‌ای Security+ بودم تا آنها را با اصول فنی این دوره آشنا و آگاه سازم (گرچه مدیران و متخصصین امنیت شبکه حُکم اساتید اینجانب را دارند، اما به حُکم وظیفه برخود لازم دانستم که این آگاه سازی را انجام دهم). اساس کتاب حاضر برگرفته از کتاب‌ها و منابع معتبر و استاندارد شاخه امنیت شبکه، مدیریت امنیت شبکه، مدیریت امنیت اطلاعات و ارتباطات، استانداردهای امنیت اطلاعات، نفوذگری و دوره Security+ می‌باشد که با تجربیات اینجانب در امر شبکه، امنیت شبکه و نفوذگری آمیخته شده است، که به فرم کاملاً آزاد از مطالب و تجربیات گردآوری، و دخل و تصرفی نیز با آن همراه بوده است. پیشاپیش تمام کاستی‌های آن را می‌پذیرم و

ضمن پوزش از اساتید، متخصصان، دانشجویان و مدیران عزیز، انتقادات و راهنمایی‌های دلسوزانه آنها را به دیده منّت پذیرا هستم.

( m_Davari@TOP-co.ir )
( m_Davary@Parshack.zzn.com )

لازم به‌ذکر است که کتاب مذکور دقیقاً برپایه مراجع و منابع مبتنی بر دوره پایه‌ای CompTIA Security+ نوشته شده است و در آن مفاهیمی چون حملات برعلیه شبکه‌ها و سیستم‌ها، نرم‌افزارهای مُخرب به‌فرم کاملاً کلی بیان شده است و جزییات آن‌ها بیان نگردیده است. وجود کتابی چون "مرجع کامل حملات هکری و طریقه مقابله" در بازار کتاب که به بررسی جزئی و کامل این مطالب پرداخته است، دلیلی شد تا از وجود مطالب تکراری در این کتاب اجتناب شود و به مطالب کلی و پایه‌ای همانند استاندارد Security+ بسنده گردد. حال درصورت نیاز به بررسی جزیی این مفاهیم می‌توانید به کتاب "مرجع کامل حملات هکری و طریقه مقابله" مراجعه نمایید تا به‌طور کامل با جزییات و ساختارهای آن‌ها آشنا شوید.

پس از سپاس و ستایش به درگاه پروردگار از تمام دوستان و اساتید عزیزی که مهربانانه دست مرا در انجام اینکار ناچیز فشردند، تشکر می‌کنم. برخود لازم می‌دانم از زحمات بی‌دریغ سرکار خانم مهندس سیده پونهٔ مرتضویان تشکر و قدردانی نمایم. زحمات خاضعانهٔ ایشان سهم بزرگی در تهیه و تدوین این کتاب داشته است.

در پایان از مدیریت فرزانهٔ انتشارات پندار پارس، جناب آقای مهندس حسین یعسوبی و تمامی همکارانشان که زحمت چاپ کتاب را متقبل شده اند، صمیمانه قدردانی می‌نمایم.

یارب ز کرم دری برویم بگشا
راهی که درو نجات باشد بنما
مستغنیم از هر دو جهان کن به کرم
جز یاد تو هرچه هست بر از دل ما

( مجید داوری دولت آبادی – زمستان ۱۳۸۹ )

# فصل اول

## مفاهیم اساسی امنیت

## مقدمه

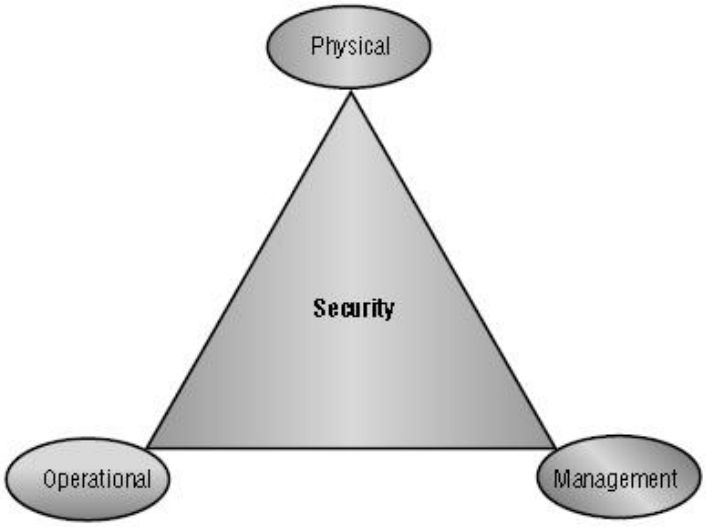
امروزه شاهد گسترش حضور کامپیوتر در تمامی ابعاد زندگی خود هستیم. کافی است به اطراف خود نگاهی داشته باشیم تا به صحت گفته مذکور بیشتر واقف شویم. هم زمان با گسترش استفاده از کامپیوترهای شخصی و مطرح شدن شبکه‌های کامپیوتری و به دنبال آن اینترنت (بزرگ‌ترین شبکه جهانی)، حیات کامپیوترها و کاربران آنها دستخوش تغییرات اساسی شده است. استفاده‌کنندگان کامپیوتر به منظور استفاده از دستاوردها و مزایای فناوری اطلاعات و ارتباطات، ملزم به رعایت اصولی خاص و اهتمام جدی به تمامی مؤلفه‌های تأثیرگذار در تداوم ارائه خدمات در یک سیستم کامپیوتری می‌باشند. امنیت اطلاعات و ایمن‌سازی شبکه‌های کامپیوتری از جمله این مؤلفه‌ها می‌باشد که نمی‌توان آن را مختص یک فرد و یا سازمان در نظر گرفت.

## مفهوم امنیت اطلاعات

امروزه شاهد گسترش حضور کامپیوتر در تمامی ابعاد زندگی خود هستیم. کافی است به اطراف خود نگاهی بیندازیم تا به‌صحت این مطلب بیشتر واقف شویم. هم‌زمان با گسترش استفاده از کامپیوترهای شخصی و مطرح شدن شبکه‌های کامپیوتری و در پی آن اینترنت، زندگی کاربران دستخوش تغییرات اساسی شده است. استفاده‌کنندگان کامپیوتر به‌منظور استفاده از دستاوردها و مزایای فناوری اطلاعات و ارتباطات، ملزم به‌رعایت اصولی خاص هستند و باید به تمامی مولفه‌های تأثیرگذار در تداوم ارائه خدمات در یک سیستم کامپیوتری توجهی جدی داشته باشند. امنیت اطلاعات و ایمن‌سازی شبکه‌های کامپیوتری از جمله این مولفه‌ها است که نمی‌توان آن را مختص یک فرد و یا سازمان در نظر گرفت. در این فصل قصد داریم به بررسی مبانی و اصول اولیه امنیت اطلاعات و ایمن‌سازی شبکه‌های کامپیوتری بپردازیم و از این رهگذر با مراحل مورد نیاز به منظور حفاظت شبکه‌ها و سیستم‌ها در مقابل حملات، بیشتر آشنا شویم. حال به‌طور کلی می‌توان امنیت اطلاعات را در سه قالب کلی پیاده‌سازی کرد. در واقع این سه قالب اساس کار امنیت اطلاعات در هر سازمان و شبکه‌های کامپیوتری مستقر در آن سازمان است. قالب‌های اشاره شده شامل موارد زیر می‌باشند:

- امنیت فیزیکی
- امنیت عملی
- سیاست‌ها، روال‌ها و اقدامات مدیریتی

برخی کتاب‌ها این سه اصل را پایه‌های اصلی امنیت می‌دانند و نقض شدن هریک از آنها موجب ایجاد اختلال در روند عملکرد و ساختار امنیت اطلاعات در شبکه‌ها و سازمان‌ها می‌شود. شکل ( ۱-۱ ) مثلث ایجاد شده برپایه این ساختار را نشان می‌دهد.




شکل ( ۱-۱ ) مثلث امنیت براساس قالب‌های کلی

## امن‌سازی محیط‌های فیزیکی

پیشرفت گسترده و روزافزون ارتباطات و فناوری‌های جدید، گرچه باعث شده است که تمرکز در به‌کارگیری تجهیزات و پایانه‌های کامپیوتری کاهش یابد و بیشتر استفاده‌کنندگان از راه دور به اطلاعات دسترسی پیدا کنند، اما هنوز هم امنیت در محیط‌های کامپیوتری از اهمیت بالایی برخوردار است. تردد افراد به مراکز کامپیوتری بسیار کمتر شده است، اما درحال حاضر نیز بایستی در طرح‌ریزی یک مرکز کامپیوتری نکات بسیاری را مدنظر قرار داد، که برخی از آنها به قرار زیر می‌باشند:

- محل استقرار تجهیزات
- مشخصات و ویژگی‌های سایت
- سیستم‌های هشداردهنده حریق و اطفاء حریق
- سیستم‌های پشتیبانی و جایگزین نیروی برق
- سیستم‌های تهویه و جایگزین آن
- وضعیت جغرافیایی (از نظر باران‌های فصلی، بادخیز بودن، سیل، زلزله و...)
- کف مرکز کامپیوتری
- سقف مرکز کامپیوتری
- محل ورود افراد

حفاظت فیزیکی اولین اصل در رعایت امنیت یک شبکه، ایجاد یک شبکه امن و رعایت اصول امنیتی کامپیوترها به ویژه سرویس‌دهنده‌های شبکه می‌باشد. از نظر کارشناسان امنیت شبکه حفاظت

از محل سرور و تعیین سیاست‌های خاص جهت دسترسی فیزیکی افراد مختلف به سرور بسیار حائز اهمیت است. اگر یک نفوذگر یا سارق الکترونیکی بتواند به‌طور فیزیکی به سرورها دسترسی پیدا کند، یعنی اینکه از طریق صفحه کلید و یا سایر دستگاه‌های ورودی با سیستم ارتباط برقرار نماید، امکان شکسته شدن موانع امنیتی بسیار زیاد خواهد بود و درصورتی که نتواند به اطلاعات دسترسی پیدا کند حداقل کاری که می‌تواند انجام دهد خاموش کردن سرور و درنتیجه از کار انداختن سرویسی است که سرور مربوطه به شبکه می‌دهد، می‌باشد.

محل قرار گرفتن سرور معمولاً باید محل ویژه و آماده شده برای این کار باشد، علاوه بر اینکه این محل باید دارای موانع مطمئن جهت جلوگیری از نفوذ افراد مختلف به آن باشد، ضمناً بایستی دارای دستگاه‌های کنترل دما و تهویه مناسب نیز باشد، زیرا ممکن است در اثر بالا رفتن حرارت در این اتاق، سرورهای مستقر در آن از سرویس خارج شوند. ضمناً بایستی سیستم‌های ضدسرقت و ضدحریق در این مکان‌ها فعال باشد. امروزه در دنیا برای امنیت این اتاق‌ها تدابیر بسیار زیادی در نظر گرفته می‌شود و هزینه بسیار زیادی نیز صرف می‌گردد. بیشتر اتاق‌های سرور را شبیه یک گاو صندوق می‌سازند و درب‌های ورودی آن بسیار مستحکم و دارای رمزهای عبور از نوع دیجیتال، صوتی و یا حساس به اعضای بدن اشخاص می‌باشد، اما گذشته از امنیت اتاق سرور برای خود سرورها نیز شرایط خاصی در نظر گرفته می‌شود، از جمله اینکه معمولاً این سرورها کلید روشن و خاموش ندارند و یا حداقل اینکه در دسترس نیستند. ضمناً بعد از تنظیم و نصب این سرورها کلیه دستگاه‌های ورودی و انتقال اطلاعات از قبیل صفحه کلید، فلاپی دیسک، CD و غیره را از آن جدا می‌کنند تا سارقین نتوانند جهت نفوذ به سرور از آنها استفاده کنند.

همان‌طور که ذکر شد اولین قدم در بحث امنیت شبکه‌ها حفظ امنیت فیزیکی آن است این موضوع زمانی بیشتر اهمیت پیدا می‌کند که بدانید هفتاد درصد حملاتی که بر علیه شبکه‌ها رخ داده است و باعث ضرر و زیان در آنها گردیده است، از داخل شبکه بوده است. استحکام فیزیکی، محلی که تجهیزات در آن قرار دارد، از نفوذ غیرقانونی جلوگیری می‌کند. موانع متعدد فیزیکی به جلوگیری از ورود و تشخیص نفوذگران کمک به سزایی می‌نمایند. در این خصوص نکات زیر را بایستی مدنظر داشت:

۱. تعیین دقیق محیطی که باید امنیت آن تأمین شود.
۲. شناسایی ضعف‌ها و آسیب‌پذیری‌ها با انجام تجزیه و تحلیل خطر
۳. حصول اطمینان از استحکام دیوارها و اینکه ورود تنها از طریق درب‌ها امکان‌پذیر است.
۴. استفاده از کف و سقف غیرکاذب به طوری که تهدیدهای فیزیکی در معرض دید باشد.
۵. کنترل دسترسی با وسایلی از قبیل کارت‌های هوشمند، دوربین و غیره
۶. زنگ خطر جهت اعلام دود، حرارت، رطوبت و ورود غیرمجاز

زمانی که ناحیه‌ای رسماً به عنوان ناحیه امن اعلام شد، تمهیدات حفاظتی برای دسترسی مجاز به آن ناحیه در نظر گرفته می‌شود. این تمهیدات به قرار زیر می‌باشند:

۱. مراجعین بایستی حتماً تا مقصد همراهی شوند و جزئیات ورود و خروج آنها ثبت گردد.
۲. استفاده از برچسب شناسایی
۳. تنها به کارمندان مجاز اجازه دسترسی به تجهیزات داده شود.
۴. بازبینی منظم حق دسترسی به نواحی امن برای اعمال تغییرات شغلی و غیره

درخصوص حفاظت از جایگاه مرکز داده‌ها و کامپیوترها بایستی به موارد زیر توجه داشت:

۱. نباید در معرض حوادث طبیعی یا غیرطبیعی مانند آتش‌سوزی، سیل و انفجار و غیره باشد.
۲. باید تا حد امکان نامشهود باشد.
۳. محل تجهیزات کامپیوتری نباید مشخص باشد.
۴. مواد خطرناک باید در فاصله مناسبی از جایگاه نگهداری شوند.
۵. تجهیزات پشتیبانی و ذخیره باید در فاصله امنی قرار گیرند تا از خرابی هم زمان جلوگیری شود.
۶. وسایل ایمنی باید به‌طور منظم کنترل شود.
۷. دستورالعمل وضعیت اضطراری باید مستند شده و به‌طور منظم آزمایش شود.
۸. درب‌ها و پنجره‌ها همواره باید قفل شوند و پنجره‌ها حفاظ داشته باشند.
۹. دیوار خارجی جایگاه باید استحکام کافی داشته باشد.

اعمال محدودیت در دسترسی به کامپیوترها و منابع اطلاعاتی مرتبط به آن, ابتدایی‌ترین شکل از امنیت کامپیوتری محسوب می‌شود. این نوع از امنیت، گرچه حفاظت فیزیکی را نیز شامل می‌گردد، اما محدود به آن نمی‌شود. پیچیده‌ترین سیستم‌های کنترل دسترسی فیزیکی به اطلاعات نیز در نهایت, پس از تلاش‌های لازم و صرف زمان کافی قابل رخنه هستند. کلیه متخصصین به این نکته آگاه هستند می‌توان دسترسی را بغرنج نمود، اما نمی‌توان آن را غیرممکن ساخت. زمانی که صحبت از امنیت کامپیوتری می‌شود، ابتدا امنیت فیزیکی در ذهن افراد نقش می‌بندد, بسیاری از روش‌های امنیت فیزیکی, روش‌هایی سنتی برای امنیت محسوب می‌شوند. قفل‌ها, حفاظ‌ها, سدها و مرزها، تمامی مواردی که موجب محدود کردن دسترسی به کامپیوترها و اطلاعات ذخیره شده در آنها می‌شوند، ابزارهای سنتی جهت فراهم آمدن امنیت فیزیکی به حساب می‌آیند. جهت به وجود آوردن امنیت فیزیکی مناسب و کافی، بایستی از ابزارها و روش‌های سنتی، بسیار فراتر رفت. کلیدهای الکترونیکی و دوربین‌های ویدئویی می‌توانند رویدادهای یک محیط کامپیوتری را ثبت کنند و جایگزین یک نگهبان گردند. روش‌های اِعمال امنیت فیزیکی بایستی به‌گونه‌ای باشند که محیط را در مقابل حوادث غیرمترقبه، خطاها و خرابی‌ها محافظت کنند. امنیت فیزیکی می‌تواند سه منظور عمده زیر را فراهم سازد:

- دسترسی به تجهیزات و داده‌ها را کنترل کند. درب‌های بسته, رمزهای ورود و روش‌های مشابهی برای محدود کردن دسترسی, از ورود افراد غیرمجاز به محوطه‌های حساس امنیتی جلوگیری می‌کند و مانع دستیابی آنها به اطلاعات ارزشمند می‌گردد.
- از سایت کامپیوتری به خصوص ساختمان و محیط محافظت کند.
- کامپیوترها و تجهیزات جانبی را در قبال بروز حوادث غیرمترقبه محافظت کند. این حوادث شامل دسترسی‌های غیرعمدی افراد غیرمجاز و ناوارد نیز می‌گردد.

با توجه به پیشرفت فناوری، امروزه دیگر کامپیوترها، پایانه‌ها و اطلاعات در اتاق‌های در بسته متمرکز نیستند و این خود باعث می‌شود که امنیت فیزیکی و اِعمال محدودیت‌های دسترسی شکل دیگری به خود بگیرد. دیگر نمی‌توان با تمرکز تجهیزات و پرسنل در اتاق‌های در بسته و کنترل ورود و خروج از دسترسی غیرمجاز به اطلاعات کاملاً جلوگیری کرد. دیسکت‌ها، نمونه بارزی از این تغییر و تحولات در تجهیزات کامپیوتری هستند که با حجم کوچک خود می‌توانند، مقادیر بسیار زیادی از اطلاعات را به راحتی از یک مرکز جمع‌آوری اطلاعات, خارج کنند، بدون اینکه به چشم بیایند. سیستم امنیت فیزیکی حاکم بر یک سازمان بایستی داده‌ها را هم مانند تجهیزات در قبال آسیب‌های فیزیکی محافظت کند.

### ○ تقسیم‌بندی امنیت فیزیکی

اکثر روش‌های امنیت فیزیکی دارای این ویژگی هستند که به طریقی بین افراد مجاز و غیرمجاز تمایز قائل می‌شوند. سه روش ساده جهت متمایز ساختن این افراد وجود دارد که به قرار زیر می‌باشند:

- براساس آنچه فرد می‌داند، مانند رمز ورود، اسم خاص و یا شماره شناسایی
- براساس آنچه فرد دارد، مانند کارت شناسایی، کارت هوشمند و یا کارت مغناطیسی
- براساس آنکه فرد چه کسی است، مانند اثر انگشت، تشخیص صدا، امضاء فرد و یا شبکیه چشم

در هر سه روش ذکر شده محدودیت‌هایی به چشم می‌خورد. به عنوان مثال در روش اول مفید بودن روش، بستگی به افراد و میزان تمایلشان نسبت به حفظ رمز اختصاص یافته به ایشان دارد و روش سوم بسیار هزینه بر و پرخرج است. جهت داشتن یک امنیت فیزیکی مناسب حداقل دو روش از سه روش مذکور بایستی به کار برده شوند. به عنوان مثال برای گرفتن پول از عابر بانک وجود کارت شناسایی به همراه رمز معتبر، مورد نیاز است. امنیت فیزیکی, علاوه بر تشخیص افراد مجاز و غیرمجاز، حفاظت از تجهیزات و داده‌ها را نیز در مقابل بلایای طبیعی و خسارت عمدی و غیرعمدی انسانی عهده‌دار است، به همین منظور سیستم‌های حفاظتی متعددی باید به کار برده شوند که به قرار زیر می‌باشند:

- سیستم‌های اطفاء و اعلام حریق, شامل زنگ‌های اخبار, دستگاه‌های آتش خاموش کن دستی و اتوماتیک، ساختمان‌های ضدحریق و دستگاه‌های تشخیص‌دهنده دود و حرارت

- سیستم‌های کنترل آب، مانند روکش‌های ضد آب تجهیزات، سقف‌های ضد آب و کف‌های زه‌کشی شده
- سیستم‌های حرارتی و تأسیساتی مناسب جهت ایجاد شرایط نگهداری مناسب محیطی تجهیزات
- سیستم‌های پشتیبان

### ○ شناسایی تهدیدها و ملاحظات محیطی

اولین قدم جهت مقابله با حوادث غیرمترقبه تشخیص تهدیدها است. در این صورت می‌توان برنامه و طرح مقابله با خطرات احتمالی مناسبی پیاده‌سازی کرد. مهم‌ترین بلایایی که می‌تواند متوجه یک سیستم کامپیوتری شوند، به قرار زیر می‌باشند:

- آتش‌سوزی
- قطع و یا نوسانات نامناسب برق
- تأثیر منابع برق و حوزه‌های مغناطیسی خارجی
- وقفه در جریان آب، گاز و تهویه
- بُروز اشکالات مکانیکی
- اغتشاش
- عواقب بلایای مذکور می‌تواند منجر به نتایج زیر گردد:
- از دست دادن سوابق تجاری حیاتی، مانند حساب‌های دریافتی، سفارشات مشتریان یا طرح‌های توسعه محصولات
- از دست دادن سیستم‌های ارتباطی
- بروز مشکلات احتمالی در سیستم‌های ایمنی کامپیوتری
- عدم امکان استفاده از برنامه‌های مهم و اساسی
- انجام عملیات با کیفیت و کارآیی پائین‌تر از حد عادی در یک مدت زمان طولانی

درنهایت مراحل مختلف رویارویی با حوادث به ترتیب زیر می‌باشد:

۱. وقوع حادثه
۲. عکس العمل آنی
۳. تشخیص نقاط آسیب دیده
۴. برگشت به حالت عملیاتی
۵. بازیابی کامل

### ○ بلایای طبیعی و حوادث غیرمترقبه

هیچ مکانی از گزند حوادث طبیعی در امان نیست. نجات یافتن از آسیب‌هایی که توسط بلایای طبیعی (مانند سیل، زلزله، آتش‌سوزی و غیره) به محیط‌های کامپیوتری وارد می‌آید، تنها به این

موضوع بستگی دارد که چگونه و تا چه حد وقوع چنین حوادثی پیش‌بینی شده است و برنامه بازیابی و جبران خسارات ناشی از این حوادث تا چه حد دقیق و کافی می‌باشد. یک بلا و مصیبت ممکن است خیلی بیش از آنچه قابل تصور باشد، آسیب برساند، تصور عدم وجود سیستم کامپیوتری یک بانک تجاری که اکثر عملیات جاری آن با استفاده از کامپیوتر انجام می‌گیرد، تقریباً غیرممکن است. در چنین مواردی وجود امکانات جایگزین و نسخه‌های پشتیبان نقش به سزایی بازی می‌کنند.

- **برنامه‌ریزی جهت مقابله با حوادث غیرمترقبه**

برنامه‌ریزی جهت مقابله با حوادث و بلایای غیرمترقبه، نوعی بیمه به شمار می‌آید. از جمله روش‌های گوناگون که می‌توان با بلایای طبیعی مقابله کرد، به قرار زیر می‌باشند:

- از وقوع آن اجتناب کرد. این روش مؤثرترین و ساده‌ترین راه جهت حفاظت از تجهیزات و داده‌ها در مقابل خطرات قابل پیش‌بینی است. یک برنامه امنیتی خوب بهترین نقش را در مقابله با چنین حوادثی بازی می‌کند.
- چنانچه غیرقابل اجتناب است، اثرات جانبی آن را کاهش داد. همیشه امکان اجتناب از وقوع برخی حوادث وجود ندارد، اما با پیش‌بینی‌های لازم می‌توان خسارات ناشی از وقوع آن را کاهش داد. (مانند زلزله)
- حوادث، علی‌رغم همه تلاش‌ها ممکن است پیش آیند، پس بایستی خسارات ناشی از حوادث را کنترل کرد.
- چنانچه همه اقدامات با شکست مواجه شد بایستی آموخت که با وجود همه مشکلات به فعالیت ادامه داد. همواره بایستی یک طرح آماده جهت مقابله با پیشامدهای احتمالی وجود داشته باشد که فوراً بتوان آن را به اجرا در آورد. چنانچه محدودیت تأمین بودجه وجود داشته باشد، بایستی روی منابعی که به سختی جایگزین می‌شوند، متمرکز شد.

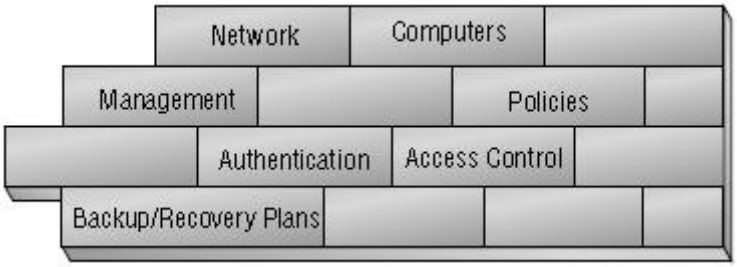
استانداردهای زیر بایستی در مورد امنیت فیزیکی مدنظر قرار داشته باشند:

۱. محل استقرار تجهیزات شبکه باید از خطراتی از قبیل سیل، گرد و غبار، لرزش و غیره در امان باشد.
۲. دمای هوا و رطوبت باید کنترل شود.
۳. تغذیه سیستم بایستی از طریق تجهیزات UPS صورت گیرد.

## بررسی امنیت عملی

اجرای امنیت عملی در یک سازمان از ارکان اصلی پیاده‌سازی صحیح امنیت در آن سازمان است. درصورتی‌که در یک سازمان امنیت عملی به‌درستی انجام نشود و اصول ان رعایت نگردد، ممکن است موجب اختلالات جدی در روند عملکرد کلی سازمان گردد، زیرا عدم رعایت حقوق پرسنل شرکت و روال‌های استخدام و اخراج ممکن است باعث نارضایتی کارمندان سازمان خواهد شود، که همین امر می‌تواند شروع یک حملهٔ الکترونیکی برعلیه سازمان مذکور باشد. زیرا براساس آمارهای گرفته شده

برخی از حملات الکترونیکی برعلیه تجارت یک سازمان توسط کارمندان ناراضی و اخراجی صورت گرفته است. درحالت کلی امنیت شامل ابزارهای مختلفی است که پیاده‌سازی این ابزارها در کنار یکدیگر کاری مشکل و نگهداری و حفظ آنها دشوارتر می‌باشد. ساختار کلی ابزارهای امنیت عملیاتی در قالب شکل (۲-۱) نمایش داده شده است.




شکل ( ۲-۱ ) ابزارهای مخصوص جهت پیاده‌سازی امنیت عملی

## طرز عملکرد سیاست‌ها و مدیریت‌ها

در دنیایی که وجه مشخصه آن فناوری سطح بالا و ارتباطات گسترده می‌باشد، هر سازمانی نیاز به سیاست‌های امنیتی که مدبرانه تدوین شده باشند دارد. در هر لحظه خطرات مختلفی از بیرون و درون سازمان توسط نفوذگران، رقبا و یا کشورهای خارجی منافع سازمان را تهدید می‌کند. هدف سیاست‌های امنیتی تعریف روال‌ها، راهنماها و تمریناتی است که امنیت را در محیط سازمان برقرار و مدیریت می‌نماید. با اجرای دقیق سیاست‌های امنیتی، سازمان‌ها می‌توانند تهدیدات را کاهش دهند. سیاست امنیتی یک سازمان سندی است که برنامه‌های سازمان برای محافظت سرمایه‌های فیزیکی و مرتبط با فناوری ارتباطات را بیان می‌کند. به سیاست امنیتی به عنوان یک سند زنده نگریسته می‌شود، بدین‌معنا که فرآیند تکمیل و اصلاح آن هیچ گاه متوقف نمی‌شود و متناسب با تغییر فناوری و نیازهای کاربران به روز می‌گردد. چنین سندی شامل شرایط استفاده مجاز کاربران، برنامه آموزش کاربران برای مقابله با خطرات، توضیح معیارهای سنجش، روش سنجش امنیت سازمان، بیان رویه ارزیابی مؤثربودن سیاست‌های امنیتی و راه کار به‌روزرسانی آنها می‌باشد.

هر سیاست امنیتی، مشخص‌کننده اهداف امنیتی و تجاری سازمان است، اما در مورد راه کارهای مهندسی و پیاده‌سازی این اهداف، بحثی نمی‌کند. سند سیاست امنیتی سازمان باید قابل فهم، واقع بینانه و غیرمتناقض باشد، علاوه بر این از نظر اقتصادی امکان‌پذیر، از نظر عملی قابل انعطاف و متناسب با اهداف سازمان و نظرات مدیریت آن، سطح محافظتی قابل قبولی را ارائه کند. بهترین روش جهت دستیابی به امنیت اطلاعات، فرموله کردن سیاست امنیتی است. مشخص کردن سرمایه‌های اصلی که باید امن شوند و تعیین سطح دسترسی افراد (به عبارت دیگر اینکه چه افرادی به چه سرمایه‌هایی دسترسی دارند)، در اولین گام باید انجام شود. هدف اصلی از سیاست امنیتی این است که کاربران

بدانند مجاز به چه کارهایی هستند. از سوی دیگر مدیران سیستم و سازمان را در تصمیم‌گیری برای پیکربندی و استفاده از سیستم‌ها یاری رساند. جهت تدوین سیاست امنیتی پس از تحلیل خطرات سازمان، می‌توان به روش‌هایی که دیگران برگزیده‌اند، متوسل شد. معمولاً تجارب مفیدی که قبلاً در صنایع مشابه انجام شده و نتایج خوبی از آنها به‌دست آمده است به صورت عمومی گزارش می‌شود و در قالب مقالات تخصصی ارائه می‌گردند. سازمان‌های بزرگ و متوسط برای تعریف سیاست امنیتی خود ناچار به پیروی روش بالا به پایین می‌باشند، اما برای سازمان‌های کوچک انجام این کار به روش پایین به بالا نیز امکان‌پذیر است. در این حالت از قابلیت‌های ابزارهای موجود بهره گرفته می‌شود. در شکل (۳-۱) هرم سیاست امنیتی نمایش داده شده است که بسته به مقیاس سازمان می‌توان از روش بالا به پایین و یا برعکس استفاده نمود.


شکل (۳-۱) هرم سیاست امنیتی

همان‌گونه که هرم سیاست شکل (۳-۱) نشان داده شده است، بهترین سیاست امنیتی در شرایطی تدوین می‌گردد که مدیریت سازمان سیاست کلی را ارائه نماید و یا دستور پیاده‌سازی اصول امنیتی را در سازمان صادر کند. تدوین‌کنندگان سیاست سازمان باید فعالیت خود را بر پایه اصول و استانداردهای صنعتی مانند ISO17799 و یا HIPAA انجام دهند. رویه‌ها، راهنماها و تجربیات، پایه‌ای جهت ایجاد و توسعه فناوری امنیتی در سازمان‌های مختلف هستند. محصولاتی مانند ESM، سازگاری و انعطاف سیاست را با سیاست‌ها و روال‌های امنیتی سیستم‌های‌عامل، پایگاه داده‌ها و برنامه‌های کاربردی ارزیابی می‌کنند. این ابزارها ممکن است با محیط کامپیوتری و شبکه سازمان در تعامل باشند. در ادامه این بخش به بررسی روال‌های موجود در سیاست‌های امنیتی می‌پردازیم.