فصل ۱
مفاهیم و کلیات

۱.۱ آشنایی با داده و تهدیدات آن

از زمانی که اینترنت در مقیاس جهانی در اختیار کاربران قرار گرفت، تعقیب و متوقف کردن مهاجمین هرچند همچنان امکان‌پذیر می‌باشد ولی بسیار پیچیده شده است. هر لحظه افراد زیادی را مشاهده می‌کنیم که اطلاعات آنها اعم از حساب‌های بانکی، فایل‌ها و تصاویر شخصی، کلمات عبور و دیگر موارد، به‌دلیل عدم آشنایی از نحوه استفاده صحیح و امن از اینترنت، رایانه یا گوشی هوشمند، و اهمیت ندادن به بحث امنیت به‌راحتی به سرقت می‌روند. از این‌رو حفظ امنیت داده‌ها در فضای مَجازی مانند دنیای واقعی برای همه‌ی افراد، چه در مشاغل کوچک و چه سازمان‌های بزرگ امری حیاتی است، و اطمینان از ایمن نگه‌داشتن داده‌ها برای جلوگیری از فاجعه، چه از جنبه شخصی و چه از نظر شغلی، ضروری است، اما متأسفانه به‌خاطر رفتارهای مُخرب یا غیرعمدی می‌تواند کار دشواری باشد.

به‌طور کلی امنیت اطلاعات با به کارگیری مجموعه‌ای از فرآیندهای کنترلی به‌دست می‌آید که در قالب خط‌مشی‌ها (سیاست‌ها[1])، روش‌های عملیاتی، ساختار سازمانی و نرم‌افزارهای عملیاتی برنامه‌ریزی و پیاده‌سازی می‌شوند.

---

[1] Policy

• **داده**[۲]

داده مفهومی مجرد، خام، بی‌معنی[۳] و سازمان نیافته از مجموعه‌ای از حقایق، ارقام و آمار مربوط به یک شیء است. داده به عنوان محوری‌ترین عنصر دارایی‌های اطلاعاتی یا دیجیتال، نقش راهبردی دارد که آن‌را از سایر دارایی‌های اطلاعاتی متمایز می‌کند.

• **اطلاعات**[۴]

با تحلیل و پردازش روی داده‌ها، مفهوم مفید و معناداری[۵] به نام **اطلاعات** به‌دست می‌آید که می‌توان آن‌را در حوزه‌های مختلف به کار برد، و مفهومی را به کاربر منتقل نمود. به‌عبارتی دیگر، اطلاعات، داده‌هایی است که سازماندهی و پردازش شده‌اند تا به آن معنا و زمینه بیشتری ببخشند. اگر داده‌ها را به مثابه قطعات یک جورچین (پازل) در نظر بگیرید، اطلاعات به مانند پازل تکمیل شده است که طرح نهایی را برای کاربر به تصویر می‌کشد.

• **جرایم سایبری**[۶]

مفاهیم رایانه، شبکه و امنیت داده‌ها در فضای سایبر هم‌مانند دنیای واقعی هستند، اما مکانیزم‌های پیاده‌سازی روال‌های مرتبط با آنها متفاوت است. از این‌رو جرایم سایبری به جرایمی گفته می‌شود که با استفاده از اینترنت یا رایانه برای انجام فعالیت‌های غیرقانونی، و اغلب جهت کسب منافع مالی یا مقاصد شخصی، حتی تنش‌های سیاسی بین دولت‌ها صورت می‌گیرد. جرایم سایبری طیف وسیعی از اقدامات غیرقانونی (از سرقت هویت و مهندسی اجتماعی گرفته تا تروریسم سایبری) را شامل می‌شود، و یکی از جنبه‌های مهم آن، ویژگی غیرملی یا فرامرزی بودن آن است.

• **رخنه یا هک کردن**[۷]

هک یا نفوذ به استفاده از دانش و تخصص علوم رایانه‌ای برای گرفتن دسترسی به یک سیستم رایانه‌ای بدون داشتن مُجوز گفته می‌شود، و به کسی که توانایی چنین کاری را دارد **نفوذگر**

[2]Data
[3]Insignificant
[4]Information
[5]Significant
[6]Cybercrimes
[7]Hacking

یا **هکر**[8] می‌گویند(وارد شدن به سیستم یا شکست دادن محاسبات، کنجکاوی در اطلاعات خصوصی و محرمانه از خصوصیات یک هکر است.) امروزه واژه نفوذگر در فرهنگ عامه به متخصصان امنیت رایانه اطلاق می‌شود که توانایی نفوذ برای کسب اطلاعات شخصی، سازمانی و محرمانه، و کنترل سیستم‌های رایانه‌ای برای اهداف گوناگون را دارند. این کاربرد خاص از این واژه بار منفی دارد که با شنیدن نام هکر، همیشه فردی مُخرب و سارق اطلاعات را در ذهن تداعی می‌کند و برای اشاره به چندین گروه از آنها استفاده می‌گردد.

هکرهای کلاه‌سفید[9]- به آن دسته از متخصصین شبکه و امنیت گفته می‌شوند که با رضایت مالک، به شناسایی هرگونه آسیب‌پذیری و ارزیابی امنیتی سامانه‌ها می‌پردازند. آنها برای کشف نقاط ضعف، به‌صورت قانونی به شبکه‌ها و سیستم‌ها نفوذ می‌کنند (هک اخلاقی[10]).

بسیاری از هکرهای کلاه‌سفید یا در شرکت‌های بزرگ فناوری اطلاعات نظیر مایکروسافت، گوگل، سیسکو و ... مشغول به کار هستند، و یا تحت عنوان شرکت‌های **تست نفوذ**[11] به شکل قانونی با سازمان‌ها قرارداد می‌بندند تا با رعایت کلیه اصول هک اخلاقی، شبکه‌ها و سیستم‌های امن را حفظ کنند و گزارش ارزیابی امنیتی (شامل نقاط ضعف و روش‌های بهبود و اصلاح سیاست‌ها یا ابزارهای امنیتی) را تنها در اختیار متولیان مربوطه قرار دهند.

[8] Hacker
[9] White-Hat Hackers
[10] Ethical hacking
[11] Pen Test (Penetration testing)

هکرهای کلاه‌سیاه[۱۲]- بر خلاف کلاه‌سفیدها، هکرهای مُخربی هستند که برای منافع شخصی و به قصد سؤ یا دلایل سیاسی و اجتماعی[۱۳] به سیستم‌ها و سایت‌ها حمله می‌کنند و به هر روشی که شده آنها را از کار می‌اندازند، و بنابر قوانین جرایم رایانه‌ای مجرم شناخته می‌شوند. در اغلب موارد، بخش بزرگی (۸۰ درصد) از توفیقات این قشر در نفوذ مدیون اشتباهات انسانی کاربران می‌باشد. همه‌ی آنها ویروس‌نویسان ماهری هستند، با ترفندهای خاص و اغواگری‌های مختلفی، ویروس نوشته شده خود را بر روی سیستم قربانی نصب و با نفوذ به آن، صدمات و خسارات جبران‌ناپذیری را به سیستم‌ها و سازمان‌ها وارد می‌کنند. اغلب با برنامه‌های قفل‌شکسته یا کِرَک شده[۱۴] برخورد داشته‌اید، اینها برنامه‌های پولی هستند که توسط نوعی از هکرهای کلاه‌سیاه موسوم به کِراکِر[۱۵] بدون توجه به قوانین مالکیت و حق نشر[۱۶]، به‌گونه‌ای دستکاری شده‌اند که بتوان از آنها به‌صورت رایگان استفاده نمود!

هکرهای کلاه‌خاکستری[۱۷]- این قشر از هکرها، بین کلاه‌سفیدها (نفوذگران قانونی) که امنیت سیستم‌ها را حفظ می‌کنند و کلاه‌سیاه‌ها (مجرمان واقعی) که برای سؤاستفاده از آسیب‌پذیری‌ها، به‌طور مُخرب عمل می‌کنند، قرار دارند. آنها برای گسترش آگاهی عمومی، در مورد وجود آسیب‌پذیری امنیتی، ناخواسته با فراهم کردن امکان استفاده برای هکرهای کلاه‌سیاه، مورد سؤاستفاده قرا می‌گیرند. در مقابل، یک هکر کلاه‌سفید ممکن است این‌کار را به‌صورت خصوصی انجام دهد و بدون اینکه نتایج را عمومی کند، به شرکت هشدار می‌دهد. هکرها در حملات خود از ابزارهایی استفاده می‌کنند که با لایه‌های دفاعی و امنیتی موجود در شبکه و یا سیستم قربانی قابل تشخیص نباشند. بدافزارها، فیشینگ[۱۸]، مهندسی اجتماعی و هر نقطه ضعف موجود در سیستم قربانی، تمام این عوامل به‌طور یک‌پارچه زمینه‌ای را فراهم می‌کنند تا هکر بتواند به سیستم نفوذ و اقدامات مُخرب خود را به سر انجام برساند.

---

[12] Black-Hat Hackers
[13] Hacktivism (Hack + Activism), Hacktivist عمل هک یا نفوذ به رایانه‌ها برای اهداف سیاسی یا اجتماعی را هکتیویسم می‌نامند و فردی که این عمل را انجام می‌دهد، هکتیویست گفته می‌شود
[14] Crack
[15] Cracker (قفل‌شکن)
[16] Copyright
[17] Grey-Hat Hackers
[18] Phishing (Password Harvesting Fishing)

تهدیدهای کلیدی که ممکن است برای امنیت داده‌ها اتفاق بیفتند، عبارتند از:

- خرابی سیستم یا دیسک‌سخت[۱۹]، باعث آسیب فیزیکی به رسانه ذخیره‌سازی می‌شود.
- دیسک‌ها و دیسک‌گردان‌های[۲۰] معیوب، مانند قطاع‌های خراب[۲۱]، که باعث بروز خسارات و آسیب فیزیکی به دیسک‌ها می‌شوند.
- ویروس‌های رایانه‌ای، که ممکن است فایل‌ها را حذف یا خراب کنند.
- از دست دادن داده‌ها[۲۲] در اثر قطع برق، حذف تصادفی یا بازنویسی اتفاقی فایل‌ها.
- حذف (عمدی) توسط کاربران غیرمُجاز یا هکرها.
- حذف تصادفی یا مُخرب توسط کارمندان (یا همکاران).
- از میان رفتن داده‌ها در اثر بلایای طبیعی مانند آذرخش (صاعقه)، سیل، زلزله و ....
- اقدامات تروریستی یا جنگی.

رایانش اَبری[۲۳]

رایانش اَبری نوعی خدمات محاسباتی مبتنی بر اینترنت است که به کاربران امکان می‌دهد بر اساس تقاضا و به وسیله‌ی شبکه، منابع و داده‌ها را در هر زمان و هر مکان با دستگاه‌های دیگر به اشتراک بگذارند. در یک محیط رایانش اَبری، خدمات، برنامه‌ها، ذخیره‌سازی و سِرورها به‌طور معمول توسط تأمین کنندگان خدمات اَبری (CSP[۲۴]) مدیریت می‌شوند. مؤسسه ملی استاندارد و فناوری (NIST[۲۵]) آمریکا، رایانش اَبری را این‌گونه تعریف می‌کند: «رایانش اَبری مدلی است برای فراهم کردن دسترسی آسان بر اساس تقاضای کاربر از راه شبکه به مجموعه‌ای از منابع رایانشی قابل تنظیم و پیکربندی (شبکه‌ها، سِرورها، فضای ذخیره‌سازی، برنامه‌های کاربردی و سرویس‌ها) که این دسترسی بتواند با کمترین نیاز به مدیریت منابع یا دخالت مستقیم تامین‌کننده سرویس، به سرعت فراهم شده یا آزاد گردد.»

[19] HardDisk
[20] Disk Drives
[21] Bad Sectors
[22] Data loss
[23] Cloud Computing
[24] CSP (Cloud Service Provider)
[25] NIST (National Institute of Standards and Technology)

نکته کلیدی در معماری رایانش اَبری، انجام خودکار بسیاری از وظایف مدیریتی است. اگر سیستم برای تخصیص منابع و فرآیندها، به مدیریت انسان وابسته باشد، دیگر اَبر نیست. در تعریف «NIST» مدل‌های استقرار اَبر از این قرارند:

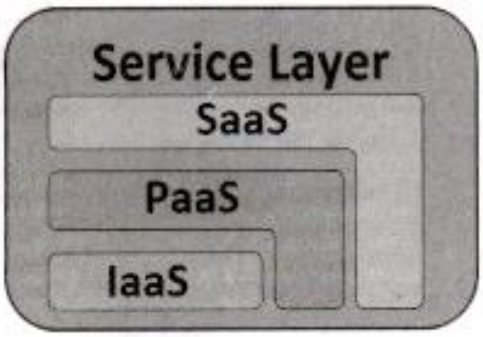
۱. اَبر عمومی[۲۶] یا اَبر خارجی[۲۷] توصیف‌کننده رایانش اَبری در معنای اصلی و سنتی آن است. خدمات و یا سرویس‌ها به‌صورت پویا و توسط اینترنت عرضه می‌شود.

۲. اَبر انجمنی یا اجتماعی[۲۸]، وقتی که چندین سازمان نیازهای یکسان دارند و به دنبال این هستند که با به اشتراک گذاشتن زیرساخت‌ها از مزایای رایانش اَبری بهره‌مند گردند.

۳. اَبر ترکیبی[۲۹] متشکل از چندین فراهم‌کننده‌ی داخلی یا خارجی می‌باشد.

۴. اَبر خصوصی[۳۰] یک زیرساخت رایانش اَبری است که توسط سازمان‌ها برای استفاده اختصاصی و داخلی خود سازمان به‌وجود آمده است.

مهاجرت به اَبر و انتخاب نوع استفاده از آن به عنوان زیرساخت[۳۱]، سکو[۳۲] و یا نرم‌افزار در قالب خدمت[۳۳]، به نتایج ارزیابی ریسک صورت گرفته از آن بخش‌ها دارد. با این حال، بهتر است بخش‌هایی که با داده‌ها یا اطلاعات حیاتی و دارای طبقه‌بندی کار می‌کنند، همچنان بر بسترهای درون سازمانی باقی بمانند.



علاوه بر امنیت داده‌ها، میزان دسترس‌پذیری و کارآیی برنامه‌های کاربردی هم که روی اَبر میزبانی می‌شوند، از اهمیت بالایی برخوردار است. اصولاً میزان از دست دادن اطلاعات در مدل اَبر به‌ویژه اَبر خصوصی نسبت به ذخیره نمودن داده‌ها در رایانه‌های شخصی یا سایر رسانه‌های ذخیره‌ساز به‌صورت محلی، به‌طور چشمگیری پایین می‌باشد.

[26] Public Cloud
[27] External Cloud
[28] Community Cloud
[29] Hybrid Cloud
[30] Private Cloud
[31] IaaS (Infrastructure as a Service)
[32] PaaS (Platform as a Service)
[33] SaaS (Software as a Service)

آسیب‌پذیری‌های رایانش اَبری

رایانش اَبری مزایا و معایب خود را دارد. پس هنگام تصمیم‌گیری برای مهاجرت به اَبر، باید برخی از آسیب‌پذیری‌های احتمالی خدمات اَبری به شرح زیر را در نظر بگیرید:

۱. **سرقت جلسه یا ارتباط رُبایی**[۳۴] - این آسیب‌پذیری زمانی رُخ می‌دهد که مهاجم، کوکی[۳۵] کاربر را در بین راه، گیر می‌آورد یا آن‌را سرقت می‌کند تا بتواند از برنامه سؤاستفاده کند. کوکی دزدیده شده به هکر این امکان را می‌دهد که هویت کاربر را جعل کند و با استفاده از اعتبارنامه تایید شده کاربر، به عنوان فرد مُجاز وارد سیستم شود.

۲. **اطمینان‌پذیری خدمات**[۳۶] - مانند خدمات محلی و اَبرهای خصوصی، باید انتظار توقف گاه‌به‌گاه و در دسترس نبودن خدمات را داشته باشید. با اینکه فراهم‌کنندگان خدمات اَبری منابع تغذیه بدون وقفه (UPS[۳۷]) دارند، اما ممکن است گاهی اوقات از کار بیفتند. بنابراین نباید انتظار فعالیت ٪۱۰۰ و پیوسته را داشت.

۳. **اتکا به اینترنت** - در دسترس بودن خدمات اَبری به شدت به پایداری و سرعت مناسب اینترنت بستگی دارد. اگر اینترنت قطع یا به‌طور موقت در دسترس نباشد، کاربران نمی‌توانند از خدمات اَبری مورد نیاز استفاده کنند و ممکن است باعث از دست رفتن درآمد شرکت شود. همچنین بر خدماتی که نیازمند فعالیت ۷×۲۴ هستند، مانند بیمارستانی که کوچکترین وقفه در پایش علائم حیاتی، جان بیمار را به خطر می‌اندازد، تأثیر می‌گذارد.

تهدیدهای رایانش اَبری

محبوبیت کار از راه دور، تهدیدات سایبری جدیدی را برای محیط‌های اَبری ایجاد می‌کند:

- **کنترل داده** – یکی از نگرانی‌های بزرگ شرکت‌هایی که به سمت اَبر حرکت می‌کنند، کنترل داده است. قرار دادن اطلاعات حساس و محرمانه سازمان بر روی سِرورهای

[34] Session Hijacking
[35] Cookie (کلوچه اطلاعات)
[36] Service Reliability
[37] UPS (Uninterruptible Power Supply)

فراهم‌کننده خدمات اَبری (CSP) خطری است که برخی شرکت‌ها تمایلی به انجام آن ندارند. چرا که نگرانند شاید امنیت داده‌هایشان به‌دست افراد ناباب بیفتد.

- **از کار انداختن یا انکار خدمات**[۳۸] – به‌دلیل فرآیند ثبت نام بسیار ساده و گاه ناشناس که برخی از CSP‌ها دارند، خدمات اَبری ممکن است برای اهداف مُجرمانه و مُخربی مانند ارسال هرزنامه[۳۹]، بات‌نِت‌ها[۴۰]، حملات انکار خدمات توزیع شده (DDoS[۴۱]) یا برای توزیع نرم‌افزارهای مُخرب مورد سؤاستفاده قرار بگیرند.

- **نقض احتمالی حریم خصوصی** – از آنجایی که خدمات اَبری از هر نقطه‌ای در اینترنت قابل دسترسی هستند، نگرانی در مورد حفظ حریم خصوصی داده‌ها وجود دارد. هنگامی که داده‌ها از کلاینت‌ها به اَبر منتقل می‌شود، مهاجم ممکن است بتواند با ارتباط رُبایی، حریم خصوصی شما را نقض کند.

- **کارمندان ناراضی**[۴۲] (نفوذی) – کارکنان CSP که می‌توانند به داده‌های شما دسترسی داشته باشند، ممکن است با رفتارهای مُخرب اطلاعات محرمانه را سرقت کنند.

- **از دست دادن داده** – این تهدید زمانی رُخ می‌دهد که دیسک‌سخت یا درایوهای CSP با مشکل مواجه شوند، و نتوانند عملیات پشتیبان‌گیری از داده‌ها را به درستی اجرا کنند، و یا CSP به‌طور تصادفی داده‌های شما را حذف کند.

حضور گسترده شرکت‌های بزرگ مایکروسافت، گوگل، آمازون، اوراکل و غیره در عرصه رقابت رایانش اَبری، نشان از توسعه سریع و تسلط این‌گونه از خدمات محاسباتی دارد.

---

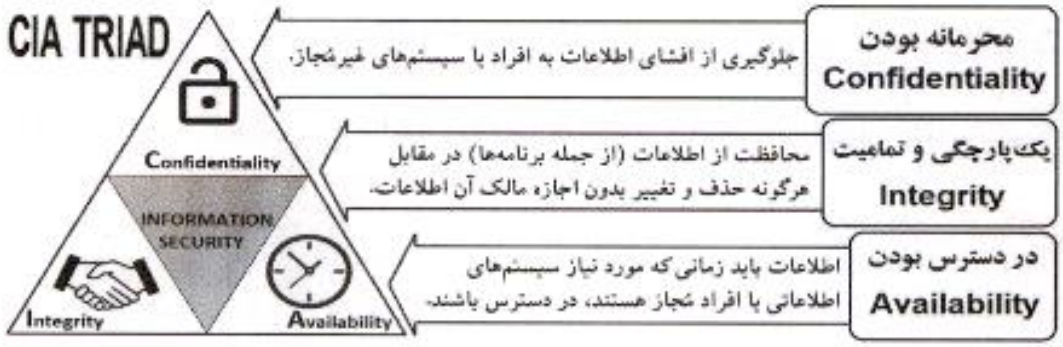
[38] DoS (Denial of Service)
[39] نامه‌های الکترونیکی ناخواسته (SPAM)
[40] Botnets (فصل ۲ را ببینید)
[41] DDoS (Distributed Denial of Service)
[42] Malicious Insiders

۲.۱ ارزش اطلاعات

اطلاعات در هزاره جدید به‌خصوص در چند سال اخیر ارزش بیشتری پیدا کرده‌اند، از این‌رو محافظت از آن نیز بسیار مهمتر شده است. گاهی اوقات شاهد استفاده از امنیت اطلاعات و امنیت سایبری به‌جای یک‌دیگر خواهید بود امنیت سایبری روشی جامع و گسترده‌تری برای دفاع از دارایی‌های فناوری اطلاعات در برابر حملات برخط است، در حالی که امنیت اطلاعات زیر چتر امنیت سایبری و به‌صورت زیرمجموعه‌ای از آن قرار می‌گیرد.

ویژگی‌های اساسی امنیت اطلاعات

امنیت اطلاعات به‌معنای محافظت از اطلاعات و سیستم های اطلاعاتی در برابر فعالیت‌های غیرمُجاز مانند: دسترسی، استفاده، افشاء، دستکاری، تغییر، خواندن، بازرسی، تخریب و نسخه‌برداری است. هدف امنیت اطلاعات، حفاظت از **محرمانگی** (یا حفظ رازداری) اطلاعات، محافظت از **یک‌پارچگی** اطلاعات و حفظ **دسترس‌پذیری** اطلاعات است.



در اصطلاحات امنیت اطلاعات، به این معیارها سه‌گانه یا مثلث CIA[۴۳] گفته می‌شود[۴۴]. وجود این سه رُکن اصلی امنیت اطلاعات در کنار هم، در سازمان‌های مختلف اساسی است اما اولویت‌بندی آنها در کسب‌وکارهای مختلف با هم متفاوت است. برای مثال، در صنعت ارتباطات و مخابرات دسترس‌پذیری از همه مهمتر است، در صنعت بانکداری و بازار پول، تمامیت و عدم تغییر اطلاعات حرف اول را می‌زند، و در سرویس‌های اطلاعاتی و امنیتی رازداری و حفظ محرمانگی در اولویت اول قرار دارد.

[43] CIA (Confidentiality, Integrity, Availability)

[۴۴] این اسم هیچ ربطی به CIA که می‌شناسیم ندارد

دلایل حفاظت از اطلاعات

امروزه بیشتر مردم از اینترنت و دستگاه‌های تلفن همراه برای خریدهای برخط، بانکداری، تجارت، ارتباطات و سایر فعالیت‌ها استفاده می‌کنند. برخی از شرکت‌ها به خدمات اَبری مختلف و سایر سرویس‌های مبتنی بر وِب برای انجام تجارت روزانه خود متکی هستند. تسهیل دسترسی به اطلاعات در اینترنت، کسب‌وکارهای این فضا را در معرض برخی مسائل امنیتی قرار می‌دهد. هکرها می‌توانند از آسیب‌پذیری‌هایی که در انتقال داده‌ها به‌صورت برخط وجود دارد، برای دسترسی غیرمُجاز به سیستم‌ها و شبکه‌ها استفاده کنند.

دلایل حفاظت از اطلاعات شخصی. هیچ چیز مهمتر از حفظ امنیت اطلاعات شخصی قابل شناسایی (PII[۴۵]) شما نیست تا بتوانید از سرقت هویت جلوگیری کنید. PII، اغلب توسط سازمان‌ها، شرکت‌ها و یا بانک‌ها برای شناسایی و اعطای مُجوز به کاربرانی که در وِب‌سایت‌های خود معاملات تجاری انجام می‌دهند استفاده می‌شود. هکرها ممکن است این اطلاعات را برای جعل هویت کاربر بدزدند و سپس به تراکنش‌های متقلبانه و غیرمُجاز و یا سایر فعالیت‌های مُجرمانه بپردازند. بدون امنیت و حفاظت کافی از اطلاعات شخصی، کاربران در معرض جرایم مبتنی بر اینترنت مانند سرقت هویت و کلاهبرداری و نقض حریم خصوصی قرار می‌گیرند. شرکت‌هایی که از اطلاعات شخصی کاربران خود محافظت نمی‌کنند ممکن است اعتماد مشتریان و جایگاه کسب‌وکار خود را از دست بدهند. چند نمونه از PII عبارتند از: نام‌ها: نام، نام خانوادگی، ...، شماره شناسایی شخصی: کُد ملی، شماره شناسنامه، شماره تلفن‌ها، شماره گذرنامه یا گواهی‌نامه، شماره حساب یا کارت بانکی، ...، تاریخ‌ها: تولد، ازدواج، آدرس‌ها: آدرس منزل و محل کار، اِیمیل، و ....

دلایل حفاظت از اطلاعات حساس تجاری. به اسرار تجاری یا هرگونه اطلاعات سازمانی[۴۶] که در صورت گم شدن یا سرقت، مورد سؤاستفاده قرار می‌گیرند و به هر نحو ممکن باعث

[45] PII (Personally Identifiable Information)

[۴۶] اطلاعات حیاتی و دارای طبقه‌بندی

بروز آسیب یا به‌وجود آمدن خسارتی به شرکت می‌شوند، اطلاعات حساس[۴۷] می‌گویند. برای نمونه، موارد زیر ممکن است به عنوان اطلاعات حساس تجاری طبقه‌بندی شوند:

- صورت‌های مالی مانند ترازنامه، صورت سود و زیان یا حقوق صاحبان سهام.
- اطلاعاتی مانند فهرست مشتریان فعلی و قدیمی، به‌خصوص مشتریان ارزنده.
- اسرار تجاری مانند طرح‌ها، فرمول‌ها، فرآیندهای تولید و غیره.
- اطلاعاتی در مورد محصولات جدید، استراتژی‌های بازاریابی یا اطلاعات ثبت اختراع.

اطلاعات حساس تجاری باید برای جلوگیری از موارد زیر محافظت شوند:

- سرقت اطلاعات خصوصی و محرمانه شرکت - اطلاعات شرکت ممکن است توسط جاسوسان، مهندسان اجتماعی یا هکرها به سرقت برود و آنها را به رقبا بدهند.
- از دست دادن تصادفی داده - کاربران ممکن است به اشتباه، داده‌های حساس را حذف یا تغییر دهند. استفاده نابجا از رسانه‌ها یا تلفن همراه حاوی اطلاعات حساس.
- استفاده متقلبانه از داده‌های شرکت - مانند اطلاعات مشتری، صورت‌های مالی.
- خرابکاری شرکتی - برخی از رقبا ممکن است از اطلاعات حساس شرکت شما برای خرابکاری و ضربه‌زدن به کسب‌وکار شما استفاده کنند.

حریم خصوصی داده[۴۸] یا کنترل حفاظت[۴۹]

اصطلاحات حریم خصوصی داده‌ها و حفاظت از داده‌ها اغلب به‌جای یک‌دیگر استفاده می‌شوند، اما تفاوت مهمی بین این دو وجود دارد. حریم خصوصی داده‌ها مشخص می‌کند که چه کسی به داده‌ها دسترسی دارد، در حالی که حفاظت از داده‌ها، ابزارها و سیاست‌هایی را برای محدود کردن دسترسی به داده‌ها فراهم می‌کند. برای حفظ حریم خصوصی، کاربران باید آن‌را کنترل کنند، اما حفاظت از داده‌ها بر عهده شرکت‌ها یا نهادهایی است که داده‌ها را مدیریت می‌کنند تا از خصوصی بودن آنها اطمینان حاصل کنند.

[47] Sensitive Information
[48] Data Privacy
[49] Protection Control

با گسترش استفاده از اینترنت برای انجام انواع مختلف تراکنش‌های تجاری و شخصی، نیاز به اقداماتی برای اطمینان از حفظ حریم خصوصی و امنیت داده‌های مورد استفاده سازمان‌ها، به‌وجود آمد. در این راستا قوانین و دستورالعمل‌هایی تدوین شدند که اطمینان بدهند، نه تنها از داده‌ها و اطلاعات سؤاستفاده نمی‌شود بلکه از آنها به‌صورت غیرقانونی هم استفاده نمی‌کنند. تدوین دستورالعمل‌های حفظ حریم خصوصی و امنیت داده‌ها، تضمین نمی‌کند که کاربران غیرمُجاز دسترسی ندارند. اما می‌توان دسترسی را با قوانین حفاظت از داده‌ها محدود کرد، و محافظت از افراد در برابر استفاده غیرقانونی از داده‌های شخصی و نقض حریم خصوصی آنها را فراهم نمود، در حالی که هنوز داده‌های حساس، آسیب‌پذیرند. به‌طور کلی، افرادی که اطلاعات شخصی در اختیار دارند باید اطمینان حاصل کنند که:

- داده‌های شخصی به شیوه‌ای عادلانه و به‌صورت قانونی[۵۰] پردازش می‌شوند.
- جمع آوری داده‌های شخصی فقط برای مقاصد قانونی که صریح بیان شده‌اند، می‌باشند.
- داده‌های شخصی اگر با هدف جمع آوری اطلاعات سازگار نباشد، پردازش نمی‌شوند[۵۱].
- داده‌های شخصی‌ای پردازش می‌شوند، که کفایت و مرتبط بودن آنها مُحرز شده‌اند.
- پردازش غیر ضروری داده‌های شخصی وجود نخواهد داشت.
- داده‌های شخصی‌ای پردازش می‌شوند که دقیق و به‌روز هستند.
- داده‌های شخصی برای مدتی بیش از زمان مورد نیاز نگه‌داری نمی‌شوند.

موضوع داده‌ها، کنترل کننده‌های داده[۵۲] و پردازشگرهای داده[۵۳]

اتحادیه اروپا (EU[۵۴])، قانونی به نام مقررات عمومی حفاظت از داده‌ها (GDPR[۵۵]) دارد که برای پردازش داده‌های شخصی و یا PII استفاده می‌شود. از سال ۱۳۹۷ (۲۰۱۸-م) اجرایی شده است و به‌طور قابل توجهی بر کسب‌وکارهای کشورهای عضو تأثیر گذاشته است.

---

[50] Lawful
[51] به این تناسب (Proportionality) گفته می‌شود
[52] Data Controllers
[53] Data Processors
[54] EU (Europran Union)
[55] General Data Protection Regulation

موضوع داده[۵۶]، هرگونه اطلاعات مربوط به فرد است، که بتوان از راه PII یا روش‌های مشابه، او را به عنوان شخصی حقیقی شناسایی کرد. موضوع داده فقط انسان‌های زنده هستند که شما اطلاعات مربوط به کسب‌وکار و فعالیت‌های آنها را از خود آنها یا درباره آنها جمع‌آوری می‌کنید. این مهم است زیرا مشخص می‌کند، از چه کسی و چه چیزی باید محافظت شود. در حالی که کنترل کننده داده، نهادی است که به تنهایی یا با همکاری دیگران، با اطمینان از کفایت و مرتبط بودن داده‌ها، مسئول کنترل و حفاظت از آنها بوده و باید در راستای اهداف مقرر استفاده کند و در صورت درخواست، بتواند نسخه‌ای از داده‌های شخصی موضوع داده را بدهد. پردازشگر داده، نهادی است که تحت هدایت مالک یا کنترل کننده داده، آنها را پردازش می‌کند[۵۷]، و مسئول رازداری و ایمنی داده‌ها نیز می‌باشد.

خط‌مشی‌های فناوری اطلاعات و ارتباطات (ICT[۵۸])

خط‌مشی‌ها یا سیاست‌های ICT در واقع سندی است که سازمان یا یک شرکت آن‌را برای اطمینان از استفاده ایمن و مناسب از خدمات و اتصالات اینترنتی یا شبکه سازمانی، تنظیم و صادر می‌کند تا کارکنان یا ذی‌نفعان خود را ملزم به رعایت مقررات آنها نماید. همچنین شاید در شغلی مشغول به کار نباشید اما از خدمات آنها استفاده می‌کنید، برای مثال دانشگاه‌ها، وسایل حمل و نقل شهری و ...، که شبکه Wi-Fi عمومی دارند، خط‌مشی‌های ICT دارند که شما را ملزم می‌کنند قبل از اتصال به شبکه، از آنها پیروی کنید.

امنیت اطلاعات[۵۹]، امنیت فناوری اطلاعات[۶۰] و امنیت سایبری[۶۱]

امنیت اطلاعات، به حفاظت از داده، فارغ از نوع و شکل آن اشاره دارد. یعنی، حفاظت از داده‌هایی که چه به‌صورت الکترونیکی ذخیره شده‌اند و یا به شکل فیزیکی در گاوصندوق نگه‌داری می‌شوند. اما امنیت IT، محدود است به حفاظت از داده و دارایی‌های اطلاعاتی

[56] Data Subject, (اصطلاحی در GDPR)
[57] مانند بخش فناوری اطلاعات
[58] Information & Communications Technology
[59] Infosec (Information Security)
[60] ITsec (Information Technology Security)
[61] Cyber Security

که فقط به شکل دیجیتال نگه‌داری می‌شوند و ما را در حفظ ارکان CIA کمک می‌کند. همچنین امنیت سایبری را می‌توان به عنوان فنون و اقداماتی تعریف کرد که برای حفاظت از داده‌های دیجیتال طراحی شده‌اند، تا به‌خصوص شرکت‌ها و موسسات (دولتی) را در مقابل دسترسی‌های غیرمُجاز و حملات مُخرب به‌ویژه سازمان‌یافته محافظت نماید.

۳.۱ امنیت شخصی

مهندسی اجتماعی (SE[۶۲])

مهندسی اجتماعی در حوزه امنیت اطلاعات، به شستشوی مغزی[۶۳] افراد، که برای انجام

کارهای خاص یا افشای اطلاعات متمرکز است، گفته می‌شود. این مفهوم که تا قبل از این تنها در مباحث سیاسی و اجتماعی کاربرد داشت، در دهه‌ی ۷۰ (۹۰-م) توسط هکر افسانه‌ای، کِوین میتنیک[۶۴] به عنوان یک روش حمله، وارد حوزه فناوری اطلاعات شد. میتنیک پس از دستگیری و اصلاح رویه زندگی خود، بعدها در زمینه امنیت مشغول به فعالیت شد و کتاب معروفی با عنوان هُنر فریب (یا گول زدن)[۶۵] را در همین حوزه نوشت. بااین‌حال، در دنیای فناوری اطلاعات به هُنر هک کردن (ذهن) انسان‌ها، مهندسی اجتماعی می‌گویند و برای طیف وسیعی از فعالیت‌های مُخرب حاصل از تعاملات انسانی برای تحت تأثیر قرار دادن افراد با هدف به‌دست آوردن غیرقانونی داده‌های حساس به‌کار می‌رود. داستان اسب تروآ، یکی از جذاب‌ترین نمونه از حملات مهندسی شده اجتماعی است.

[62] SE (Social Engineering)
[۶۳] دستکاری روانشناختی یا بازی با افکار
[64] Kevin D. Mitnick
[65] THE ART OF DECEPTION, 2002, J.Wiley

مهندسان اجتماعی، به کلاهبردارانی گفته می‌شود که به‌راحتی می‌توانند حرص، طمع، حس کنجکاوی، حس اعتماد و ...، را در قربانی برای درآمد و کسب پول بیشتر یا بهره‌مندی از خدماتی که به آسانی امکان‌پذیر نباشد، تحریک کنند و پس از گرفتار شدن کاربران، اهداف شوم خود را به اجرا می‌گذارند. آنان در مورد محیط اطراف و علایق شخصی سوژه تحقیق می‌کنند، ابتدا اطلاعات لازم را به‌دست می‌آورند و سپس هویت آنها را جعل می‌کنند. اما در بیشتر موارد، انگیزه آنها از نفوذ به سیستم‌ها، برای جاسوسی از داده‌های حساس است.

مهندسی اجتماعی (فن تحریک و متقاعدسازی افراد)، تنها یکی از انواع راه‌های هک سیستم‌ها است که در آن هکرها جهت رسیدن به اهداف پلید خود از حقه‌های بشردوستانه برای جلب اعتماد استفاده می‌کنند. بنابراین در دادن اطلاعات، حساس و هوشیار باشید.

روش‌های مهندسی اجتماعی

به‌طور کلی، مهاجمان مهندسی اجتماعی یکی از دو هدف زیر را دنبال می‌کنند:

- خراب‌کاری[۶۶]، مختل کردن یا خراب کردن داده‌ها برای آسیب‌رساندن یا ناراحت کردن.
- سرقت[۶۷]، به‌دست آوردن چیزهای ارزشمندی مانند اطلاعات، حق دسترسی، یا پول.

آنچه مهندسی اجتماعی را به شکل خاصی خطرناک می‌سازد این است که به‌جای بهره‌کشی از آسیب‌پذیری‌ها در نرم‌افزار و سیستم عامل یا سخت‌افزار، متکی به خطای انسانی است[۶۸].

[66] Sabotage
[67] Theft
[68] e.g. Catch Me If You Can (2002 film)
فیلم سینمایی «اگه می‌تونی منو بگیر»

• **فیشینگ (حملات صیادی)**

فیشینگ، یکی از اغواکننده‌ترین، محبوب‌ترین و شایع‌ترین حملات مهندسی‌شده اجتماعی است که بدون هک سیستم، از فناوری‌های ارتباطی برای فریب و سرقت اطلاعات استفاده می‌کند (شبیه ماهیگیر که با نصب طعمه سر قلاب، به دنبال شکار ماهی است). اما در عمل به هر نوع گول زدن یا کلاهبرداری برای کسب اطلاعات از سوژه اطلاق می‌گردد. در این روش، مهاجم با تقلب[۶۹] آدرس وِب‌سایت یا نشانی اِیمیل، یا با جعل عنوان مقام بلندپایه یا کارشناس فنی شرکتی معروف و غیره، سعی در فریب و متقاعد کردن قربانیان، برای افشای اطلاعات شخصی یا حساسی که آنها در اختیار دارند، می‌باشد.

برای مثال، اِیمیلی با مضامین زیر دریافت می‌کنید و در آنها نوعی اضطرار و فوریتی برای انجام کاری که از شما خواسته شده است، وجود دارد. مهاجم با طرح درخواست‌های به ظاهر حساس به زمان، چنین وانمود می‌کند که اگر تعللی از سوی قربانی صورت بگیرد، فرصتی را از دست داده یا متضرر شده و با ترساندن او به‌گونه‌ای جریمه خواهد شد. در مواقع مختلف، ممکن است این پیام‌ها متنوع و حتی واقعی‌تر از نوع واقعی آن باشند!:

- ... شما برنده «مبلغ» وجه نقد از طرف بانک B شده‌اید برای دریافت جایزه، اطلاعات مورد نیاز را در لینک زیر وارد کنید. ...
- جناب آقای X با شماره تلفن T و آدرس محل سکونت Y برای جلوگیری از اِعمال جریمه برق/آب/گاز اضافی (یا خودرو) با شناسه قبض M و شناسه پرداخت N به لینک زیر مراجعه نمایید.

در حقیقت، پیوند درج شده در این‌گونه اِیمیل‌ها شما را به سایت‌های جعلی و مُخربی که بسیار شبیه به صفحات وِب قانونی هستند، می‌کشاند و تمام اطلاعات وارد شده را به مقصدی نامعلوم ارسال می‌کند. بنابراین، در چنین مواقعی باید هوشیارانه عمل کرده و بر خلاف انتظار هکر، شتاب‌زده عمل نکنید، و قبل از هر واکنشی قدری درنگ کنید.

[69] Fraud

• **فیشینگ صوتی (تخلیه تلفنی)**

به‌دلیل اعتماد مردم به تلفن، فریب توسط آن به شکل صوتی یا ویشینگ[۷۰] یکی از متداول‌ترین روش‌هایی است که مهندسان اجتماعی در حملات خود از آن استفاده می‌کنند. قبل از هر اقدامی، باید بدانید که اطلاعات شخصی یا سازمانی خود را در اختیار چه کسی قرار می‌دهید. فقط در صورتی این‌کار را انجام دهید که از طرف مقابل مطمئن باشید، یا اینکه شما تماس گرفته باشید. چون اساس تخلیه تلفنی بر غفلت و فریب است، مهاجم در این روش سعی می‌کند برای تخلیه اطلاعات از یک فرد ناآگاه، هویت اشخاص یا سازمان‌های مورد اعتماد و معتبر (مانند کارشناس فنی، مدیر عامل یا یک مقام مسئول) را جعل کرده، و اینک که قربانی را با ترفندهای روانشناسی مرعوب نموده است، بسته به نوع نیازش او را وادار به افشای رمزعبور، اطلاعات حیاتی و یا دارای طبقه‌بندی می‌نماید.

• **فیشینگ متنی (اِس‌اِم‌اِس فیشینگ یا کلاهبرداری با پیامک)**

فریب به شکل پیام متنی (SMS[۷۱]) در تلفن همراه یا در شبکه‌های اجتماعی را اِسمیشینگ[۷۲] می‌گویند. مهاجمین در این روش با ترساندن یا تطمیع قربانیان خود، از آنها می‌خواهند که اقدامات فوری و آنی را انجام دهند. پیام‌ها به‌گونه‌ای ساخته می‌شوند که شخص، مضطرب یا خیلی شوق‌زده شود. هر فردی در چنین حالات روحی، ممکن است بی‌درنگ روی پیوند اشاره شده در پیام کِلیک کند، که یا در تله وِب‌سایت تقلبی مهاجمین میفتد، یا منجر به دانلود بدافزار و یا به‌راحتی موجب تحویل و افشای اطلاعات شخصی می‌شود. حملات اِسمیشینگ، مدیون عادی شدن استفاده از برنامه‌های موبایلی برای پراخت قبوض و انجام انواع تراکنش‌های کسب‌وکاری، و همچنین احراز هویت دومرحله‌ای[۷۳] برخط که خود باعث افزایش اعتبار پیامک‌های ارسالی نزد کاربران شده است، می‌باشد. اما برخی به سختی می‌توانند تفاوت پیامک‌های معتبر و قانونی را از جعلی تشخیص دهند!

[70] Vishing (Voice Phishing)
[71] SMS (Short Message Service)
[72] SMiShing (SMS Phishing)
[۷۳] فصل ۴، «احراز هویت چند عاملی» را ببینید

• **مخفیانه نگاه‌کردن یا سَرَک کشیدن**[۷۴]

این روش به معنای ایستادن کنار فرد قربانی و استفاده از فنون مشاهده مستقیم، اما به صورت مخفیانه (یا زیرچشمی دیدزدن) از روی شانه‌ی کسی، به صفحه‌نمایش یا صفحه‌کلید او برای به‌دست آوردن اطلاعات، کُدهای امنیتی و یا گذرواژه‌ها، اشاره دارد، تا در موقع لزوم از آن سؤاستفاده کند. نمونه بارز این نوع حمله در کنار دستگاه‌های ATM[۷۵] و POS[۷۶] مشهود است. زمانی که در حال تحریر گذرواژه‌ها یا رمز کارت بانکی خود هستید، توجه اطرافیان شما هم به دکمه‌هایی معطوف است که بر روی صفحه‌کلید می‌زنید.

• **مهندسی معکوس اجتماعی**[۷۷]

در این روش به‌جای اینکه مهاجم به قربانی نزدیک شود و با او تماس مستقیم برقرار نماید، نفوذگر سعی می‌کند مخاطب را به این باور برساند که او شخص قابل اعتمادی است و به‌گونه‌ای رفتار می‌کند که قربانی وادار شود از وی کمک خواسته و به سمت او بیاید.

- کارشکنی: او این‌کار را ابتدا با ایجاد مشکل و اختلال در کار قربانی شروع می‌کند.
- بازاریابی: سپس در نقش فردی کمک‌کننده، به موقع خود را به هدف نزدیک می‌کند.
- پشتیبانی: و در آخر به حل مشکلاتی که توسط خودش به‌وجود آمده، می‌پردازد و به این ترتیب نقشه‌های پلید خود را پیش می‌برد.

سرقت هویت و پیامدهای آن

در حال حاضر، سرقت هویت به عنوان رایج‌ترین جنایت یقه‌سفید می‌باشد و زمانی است که شخصی به عمد هویت و اطلاعات حیاتی شخص دیگری را (بیشتر برای کسب منافع مالی و به شیوه‌ی مهندسی اجتماعی) جعل کرده و از آن استفاده می‌کند. برای محافظت در برابر دزدی و سایر جنایات تهدید کننده باید اطلاعات و آگاهی خود را افزایش دهیم. در حالی که رابطه بین سرقت هویت و تروریسم ممکن است کمی دور از ذهن به نظر برسد،

[74] Shoulder Surfing موج سواری شانه‌ای
[75] ATM (Atumated Teller Machine)
[76] POS (Point-Of-Sale)
[77] Social Reverse Engineering

اما واقعیت این است که سرقت هویت نقش مهمی در بسیاری از حوادث تروریستی، داشته است. پیامد اصلی سرقت هویت، متوجه خود قربانی است که باید زمان و هزینه گزافی را برای بازیابی هویت و دریافت نسخه دوم اوراق شناسایی (المثنی) صرف کند.

روش‌های سرقت هویت[۷۸] (در مهندسی اجتماعی)

- **غواصی اطلاعات[۷۹] یا زباله‌گردی[۸۰]**

شاید تعجب کنید اما زباله‌های هر سازمان بهترین محل برای کسب اطلاعات می‌باشد و نزد مهاجمان به اندازه گنج ارزشمند است[۸۱]. متاسفانه اشخاص، سازمان‌ها و یا شرکت‌ها برای از میان بردن اسناد و زباله‌های اطلاعاتی خود (از روی حافظه‌های USB، دیسک‌های سخت، رایانه‌های شخصی، تلفن‌های همراه، و ...)، از روش‌های صحیح و مناسب تخریب اطلاعات[۸۲] استفاده نمی‌کنند[۸۳]. بنابراین مهاجم با جستجو و غوطه‌ور شدن در آشغال‌ها یا زباله‌گردی، به‌راحتی می‌تواند به اطلاعات حساس و مفید بسیاری دست پیدا کند.

[78] Identity Theft
[79] Information Diving
[80] Dumpster Diving
[81] Your Trash, My Treasure
[۸۲] به صورت فیزیکی یا منطقی
[۸۳] فصل ۷ را ببینید

• **تکثیر کارت‌های حاوی نوار مغناطیسی-اِسکیمینگ**[۸۴]

سارقان هویت برای دزدیدن اطلاعاتی که در نوار مغناطیسی پشت کارت ذخیره شده است، از دستگاه الکترونیکی کوچکی به نام اِسکیمر[۸۵] که تمام اطلاعات نوار مغناطیسی کارت را می‌خواند و ذخیره می‌کند، استفاده می‌کنند، تا در فرصت مناسب توسط خود سارق یا با فروش اطلاعات، یک کارت ثانویه تولید کنند. به این روش اِسکیمینگ می‌گویند. سارقان، اِسکیمرها را با مهارت خاصی یا در شیار کارت‌خوان دستگاه‌های عابربانک (به همراه تجهیزات اضافی دوربین‌های کوچک یا صفحه‌کلید قلابی برای ثبت گذرواژه‌ها) نصب می‌کنند، یا زیر پیشخوان (موقع استفاده از POS) پنهان می‌کنند.

• **بهانه‌تراشی**[۸۶]

در این روش مهاجم از راه یک سری سناریوی ابداعی و با بهانه‌تراشی‌ها یا دروغ‌های هوشمندانه ذهن قربانی را درگیر هدف خود کرده و با جعل هویت اشخاص یا نهادهای قابل اعتماد، چنین وانمود می‌کند که به اطلاعات حساس قربانی برای انجام یک کار مهم و ضروری، نیاز فوری دارد. بهانه، این احتمال را افزایش می‌دهد که قربانی اطلاعاتی را فاش کند یا اقداماتی را انجام دهد که در شرایط عادی از او بعید است. برای مثال، شخص وانمود می‌کند از شرکتی است که به شما خدمات می‌دهند و با بهانه‌تراشی شما را متقاعد می‌کند که جزئیات حساب بانکی خود را با آنها به اشتراک بگذارید.

• **شبکه‌های اجتماعی**[۸۷]

شبکه‌های اجتماعی به‌خاطر سهولت در عضوگیری، ملاحظات امنیتی پایینی در حفاظت از حریم خصوصی دارند. سارقان هویت با ایجاد پروفایل‌های قلابی، شبکه‌های اجتماعی را برای اطلاعات شخصی، که توسط خود کاربران منتشر شده‌اند کنکاش می‌کنند تا از این اطلاعات در مهندسی اجتماعی، برای معتبر جلوه دادن فعالیت‌های بعدی، استفاده کنند.

[84] Skimming
[85] Skimmer
[86] Pretexting (Pre-texting)
[87] Social Networks

۴.۱ امنیت پرونده (فایل)

اغلب، برخی از مهمترین اطلاعاتی که دارید در پرونده‌هایی از نوع واژه‌پردازها (مانند Word (وُرد) یا Writer) و صفحات گسترده (مشابه Excel (اِکسل) یا Calc) ذخیره می‌شوند.

Linux/Mac: LibreOffice & OpenOffice (Writer, Calc, Impress, ...)

Windows: Microsoft & Microsoft Mac (Word, Excel, Powerpoint, ...)

طیف وسیعی از ملاحظات امنیتی مرتبط با این پرونده‌ها[۸۸] وجود دارند که باید از آنها آگاه باشید. در اینجا به قفل‌گذاری یا رمزگذاری[۸۹] (گذاشتن رمزعبور) به عنوان روشی برای محدود کردن دسترسی به پرونده‌ها، پوشه‌ها و درایوها می‌پردازیم، اما مفهوم رمزنگاری[۹۰] که بر پایه دانش ریاضی-آمار، نظریه اعداد و نظریه اطلاعات بنا شده است، را به «دوره پیشرفته» همین مجموعه واگذار می‌کنیم[۹۱].

فعال/غیرفعال کردن تنظیمات امنیتی ماکروها[۹۲]

ماکروها مجموعه‌ای از دستورات هستند که برای خودکارسازی کارهای تکراری یا پُرکاربرد در برنامه‌های اداری-دفتری (مایکروسافت[۹۳]) استفاده می‌شوند. یک ماکرو را می‌توان با استفاده از ویژگی ضبط ماکرو ایجاد کرد یا توسط توسعه‌دهندگان نرم‌افزار با استفاده از VBA[۹۴] نوشت. فردی با نیات پلید از این قابلیت افزوده، می‌تواند ماکروهای مُخربی ایجاد کند که قادر است بدافزارها یا ویروس‌ها[۹۵] را مخفیانه پخش کنند. بنابراین، با اینکه ماکروها خیلی مفیدند اما رفتار هکرها آنها را به یک تهدید امنیتی بالقوه تبدیل کرده‌اند.

کاربران می‌توانند ماکروها را به‌صورت خودکار غیرفعال کنند و تنها زمانی آنها را فعال کنند که به منبع فایل، اعتماد کافی داشته باشند. در برخی از سازمان‌ها، این تنظیمات به‌طور

---

[۸۸] که به‌طور گسترده در نرم‌افزارهای MSOffice، LibreOffice و OpenOffice استفاده می‌شوند

[89] Encryption

[90] Cryptography

[۹۱] امنیت فناوری اطلاعات - دوره پیشرفته

[92] Macroinstruction

[۹۳] اگر پسوند پرونده Office به m ختم شود، دارای ماکرو است (.xlsxm .pptxm .docxm .docm)

[94] VBA (Visual Basic for Applications)

[95] Malware or Viruses

پیش‌فرض غیرفعال هستند و بدون مُجوز از مدیران سیستم قابل تغییر نیستند. می‌توانید کُد ماکرو را از رایانه‌ای به رایانه دیگر (حتی به لینوکس) ببرید و در آنجا اجرا کنید، یا با دوستان خود به اشتراک بگذارید.

ماکروها، برای اساتید و معلمان: جهت ساختن آزمون‌ها،

برای صاحبان فروشگاه: جهت ایجاد و مدیریت برنامه‌های تراکنش (POS)،

برای شرکت‌ها: جهت تولید صورت‌حساب‌ها، عالی است.

برای مثال، در زیر به‌طور مختصر به نحوه استفاده و فعال کردن ماکروها در سیستم عامل‌های لینوکس/مَک و ویندوز اشاره شده است.

Calc: Tools > Organize Macros > Basic (Mac: LibreOffice > Preferences)

Excel: File > Options > Trust Center > Trust Center Settings > Macro Settings

رمزگذاری روی فایل‌ها

یکی از اقدامات امنیتی بسیار مهم که می‌تواند از به‌وجود آمدن اتفاقات بد و گاهی جبران‌ناپذیر جلوگیری کند، قفل‌گذاری برای فایل، پوشه و درایوها است. اگر هکرها بتوانند به سیستم شما نفوذ کنند، به احتمال زیاد سرقت داده و دستکاری آن، دو عمل اصلی‌ای خواهند بود که انجام می‌دهند. به همین منظور با رمزگذاری بر روی داده‌های حساس در سیستم خود، ضمن غیرقابل خواندن آنها، می‌توانید خطرات (ریسک) ناشی از دزدی و تقلب را تا حد امکان کاهش دهید.

با تنظیم و گذاشتن رمزهای عبور در برنامه‌های مجموعه اداری-دفتری (آفیس)، می‌توانید از گذرواژه‌ها برای محافظت و جلوگیری از باز کردن و اصلاح اسناد واژه‌پردازها، کاربرگ‌های اِکسل و نمایش مطالب (پاورپوینت[۹۶]) خود، توسط افراد دیگر استفاده کنید.

Calc/Writer: File> Save As...> Save with password (/Save with GPG key)

Excel/Word: File> Info> Protect Workbook/Document> Encrypt with Password

[96] PowerPoint, Impress

رمزگذاری روی پوشه‌ها و درایوها

داشتن لپ‌تاپ یا دیسک‌سخت به سرقت رفته استرس‌زا است، اما با رمزگذاری مناسب می‌توانید داده‌های خود را ایمن نگه‌دارید. رمزگذاری تنها شکل تامین امنیت در دستان شما نیست، با این‌حال فقط می‌تواند شما را در برابر تهدیدهای فیزیکی محافظت کند و ممکن است همچنان در مقابل سایر اشکال جرایم اینترنتی آسیب‌پذیر باشید. برای رمزگذاری پوشه‌ها یا درایوها، می‌توانید از قابلیت سیستم عامل یا از نرم‌افزارهای شرکت‌های ثالثی که در این زمینه فعال هستند، استفاده نمایید[۹۷].

Linux: gpg -c samplfile.txt (gpg samplfile.txt.gpg)

MacOS: Security & Privacy> FileVault> Click on LOCK icon> Turn On FileVault> Continue and Restart the system

Windows: Right-Click on Folder > Properties > General tab > Advanced > ☑ Encrypt contents to secure data

مزایا و محدودیت‌های رمزگذاری

یکی از مهمترین و اصلی‌ترین دلایل استفاده از رمزگذاری، حفظ محرمانگی است.

- مزایا:

- تضمین می‌کند که داده‌های خصوصی و محرمانه فقط توسط گیرنده مورد نظر قابل مشاهده است. یعنی، اطمینان می‌دهد فقط کسانی که مُجاز به دیدن اطلاعات هستند قادر به مشاهده آن خواهند بود، نه هیچ کس دیگری.
- رمزگذاری داده‌ها در حین انتقال، از باز کردن و خواندن داده‌ها توسط هر فردی که گیرنده مورد نظر داده نیست، جلوگیری می‌کند، حتی اگر داده رهگیری یا فاش شود.
- یک‌پارچگی داده‌ها را تضمین، و از هرگونه تغییر غیرمُجاز داده‌های شما جلوگیری می‌کند.
- رمزگذاری به شما این امکان را می‌دهد که بررسی کنید آیا مالک و نویسنده سند همان کسی است که ادعا می‌کند یا نه.

[97] VeraCrypt, Folderlock, Diskcryptor, ...

- محدودیت‌ها:

- اگر رمز عبور خود را فراموش کنید، دیگر نمی‌توانید اطلاعات خود را بازیابی کنید.
- برخی از اَشکال رمزگذاری، حفاظت را تنها به صورت اسمی دارند (مانند پرونده‌های قدیمی ZIP، سند Word یا Pdf)، که به‌راحتی می‌توانند با برنامه مناسبی شکسته شوند.
- وجود پرونده‌های رمزگذاری‌شده باعث جلب توجه کاذب می‌شود و در مورد آنچه که می‌خواهید از آن محافظت کنید، شک و شبهه ایجاد می‌کند، و این در حالی است که پرونده‌های رمزگذاری‌نشده به همان میزان، علاقه مهاجمان را به خود جلب نمی‌کند.
- نمی‌تواند از حذف داده‌ها جلوگیری کند.

با این همه، رمزگذاری به اندازه رمزنگاری مستحکم نیست. رمزنگاری فرآیندی است که با به کارگیری یک تابع ریاضی به نام کلید (که توسط الگوریتم رمز[۹۸] تولید شده است) بر روی متن نامه یا پرونده‌ها اجرا می‌شود و محتوای آن‌را برای همه غیرقابل فهم یا خواندن می‌کند، مگر اینکه کلید رمزگشایی آن‌را داشته باشیم[۹۹].

کارگاه آموزشی

۱- مواردی از اِسمیشینگ را که برای شما اتفاق افتاده است با دیگران به اشتراک بگذارید.

۲- ماکرویی برای پرونده وُرد یا اِکسل تهیه و سپس آن‌را فعال/غیرفعال کنید.

۳- روی پرونده‌های دفتری-اداری رمزگذاری کنید.

۴- سعی کنید رمزهای عبور را که بر روی پرونده‌های دفتری-اداری خود گذاشته‌اید، بشکنید!

۵- با استفاده از ابزار Folderlock پرونده‌ها و پوشه‌ها را قفل‌گذاری و مخفی کنید.

---

[98] Algorithm

[۹۹] امنیت فناوری اطلاعات - دوره پیشرفته

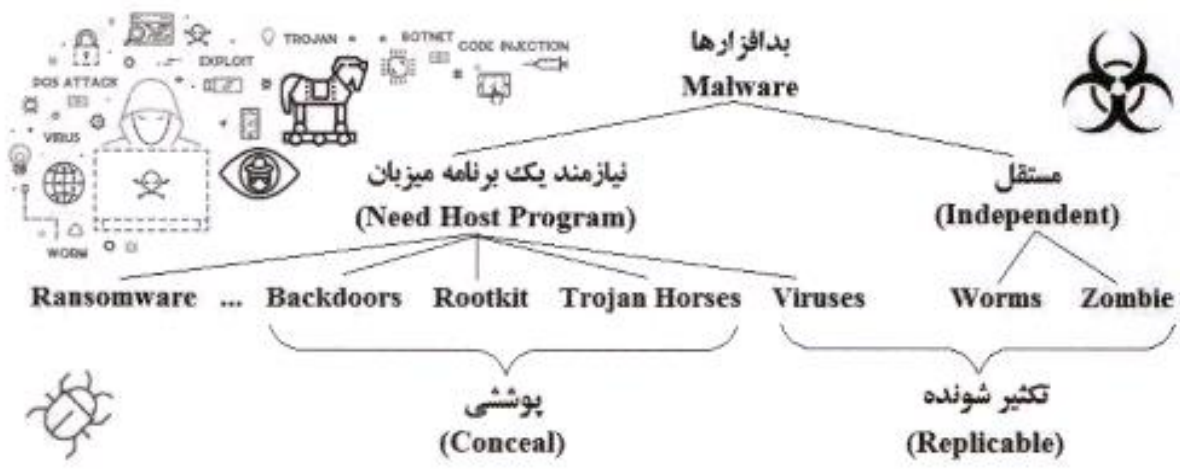
فصل ۲

بدافزار

۱.۲ انواع بدافزار

تعریف بدافزار

بدافزار، نرم‌افزار مُخربی[1] که نوشته یا طراحی شده است تا خود را بر روی رایانه یا دستگاه، بدون اطلاع و رضایت مالک، نصب و به قصد انجام کارهای ناخواسته و خراب‌کارانه (مانند انهدام و تغییر عملکرد سیستم، سرقت اطلاعات، سؤاستفاده و ...) به سیستم‌ها (-ی ناامن) نفوذ و آنها را آلوده کند. این واژه به عنوان یک اصطلاح به‌صورت چتری برای توصیف انواع مختلفی از نرم‌افزارهای مُخرب استفاده می‌شود.



[1] Malicious Software (Malware)

انواع بدافزارها

وجود تعداد بی‌شماری از برنامه‌های مُخرب و تنوع زیادی که در عملکرد آنها وجود دارد، طبقه‌بندی دقیق آنها را مشکل می‌سازد. اما تفاوت ویروس و کِرم در چیست؟ این دو چه تفاوتی با تروجان دارند؟ نشانه‌های آلودگی چیست؟ و در صورت آلودگی چه باید کرد؟

- **ویروس‌ها**

بدافزاری است که در صورت دخالت انسان می‌تواند تکثیر[۲] شود و به رایانه آسیب برساند. اصطلاح ویروس (یا سَم) رایانه‌ای از ابتکارات دانشمندان علوم رایانه است[۳]، زیرا شیوه سرایت و رفتار عفونی آنها خیلی شبیه ویروس‌های طبیعی می‌باشد.

- **کِرم‌ها**[۴]

بدافزار بسیار مُخربی می‌باشد که بر خلاف ویروس، خودتکثیرشونده[۵] است و از شبکه‌های رایانه‌ای برای ارسال نسخه‌ای از خود به رایانه‌های دیگر استفاده می‌کند.

- **تروجان‌ها**[۶]

بدافزار بسیار خطرناک و غیر خودتکثیرشونده‌ای است که همچون اسلاف تاریخی خود (اسب تروآ) در پوشش یک برنامه معتبر و قانونی و به ظاهر مهربان و معمولی (مانند بازی)، وانمود می‌کند برنامه‌ای بی‌ضرر است، اما وقتی وارد رایانه قربانی می‌شود در پشت پرده و به‌صورت غیرمستقیم، دست به اقدامات مُخرب و ویران کننده‌ای می‌زند.

- **روت‌کیت‌ها**[۷]

روت‌کیت (یا رخنه‌افزار)، بدافزاری از دسته تروجان‌ها است و سیستم عامل را به گونه‌ایی دست‌کاری می‌کند که بتواند دسترسی مداوم به رایانه‌ها یا دستگاه‌ها را امکان‌پذیر سازد، و در همان حال سعی می‌کند با مُجوز مدیریتی که دارد، حضور خود و فعالیت‌هایش (از دید کاربر) پنهان بماند و در لیست پردازش‌های سیستم اثری از او نباشد (\$ ps -ef).

---

[2] Replicate

[3] فصل ۱۲، کتاب مبانی نوین کامپیوتر، انتشارات ستایش - ۱۳۷۷، از همین مؤلف را ببینید

[4] Worms (e.g. Stuxnet)

[5] Self-replicating

[6] Trojan Horses

[7] Rootkits

- **درب پُشتی**[8]

درب پُشتی، روشی برای دور زدن احراز هویت عادی محسوب می‌شود. در واقع، درب پُشتی، بدافزاری است که به نفوذگر اجازه می‌دهد تا با دور زدن رویه‌های معمول احراز هویت (نظیر اخذ گذرواژه)، به‌صورت ناشناس به سیستم وارد شود، و به‌خاطر همین، تلاش می‌کند تا دسترسی غیرمُجاز خود از راه دور به رایانه قربانی را، ایمن‌سازی نماید. به اینها تروجان دسترسی از راه‌دور یا RAT[9] نیز می‌گویند.

انواع روش‌های سرقت اطلاعات با بدافزار[10]

در فضای مَجازی دزدی یا سرقت داده، به دسترسی غیرقانونی (خواندن، ویرایش یا کپی) داده‌ها بدون مُجوز مالک آن گفته می‌شود. داده‌ها را به شیوه‌های مختلفی می‌توان به سرقت برد. یکی از روش‌های مرسوم استفاده مهاجمان از بدافزارها، برای کسب منافع شخصی و اقتصادی است. به همین منظور، هکرها رایانه‌ها را با بدافزارها آلوده می‌سازند، تا بتوانند به طرق مختلف از آنها درآمدزایی کنند. برای آشنایی بیشتر، در زیر چند نمونه از سرقت داده‌ها با استفاده از بدافزارها و اخاذی توسط آنها، آورده شده است:

- **بات‌نِت‌ها (شبکه رُبات‌ها)**[11]

بات مخفف رُبات است و در اصطلاح فنی به یک سیستم آلوده به رُبات، بات یا زامبی[12] می‌گویند. در برخی موارد، هکرها از بات‌نِت‌ها (یعنی گروهی از زامبی‌ها) به اَشکال مختلف[13] برای ارسال حجم زیادی از درخواست‌ها و ترافیک به سمت سِرور یا وِب‌سایت هدف، استفاده می‌کنند، تا آن شبکه را از دسترس کاربرانش خارج سازند. این نوع حمله به عنوان حمله از کار انداختن یا انکار خدمات توزیع شده (DDoS) شناخته می‌شود. سپس مهاجمان در ازای توقف حمله، اقدام به اخاذی از صاحبان شرکت می‌کنند.

---

[8] Backdoor
[9] RAT (Remote Access Trojans)
[10] بدافزارهای منفعت طلب
[11] Botnets (Robot Networks)
[12] Zombie (مُرده متحرک)
[13] امنیت فناوری اطلاعات - دوره پیشرفته

- **باج‌افزارها**[۱۴]

برخی از هکرها، از نوعی بدافزار مُخرب به نام باج‌افزار استفاده می‌کنند که تمام داده‌های کاربر (روی رایانه یا تلفن همراه) را با الگوریتم‌های رمزنگاری پیشرفته، رمزگذاری کرده و دسترسی مالک را به این داده‌ها مسدود می‌کند، و برای بازگرداندن آنها به بیت‌کوین باج می‌خواهد. این امر ردیابی پرداخت‌ها و پیگرد قانونی مجرمین را بسیار دشوار می‌کند و باج‌افزار را به یک ماشین پول‌ساز تبدیل نموده است.

- **تروجان‌های بانکی**[۱۵]

تروجان بانکی نوع پیچیده‌ای از بدافزار است که به مهاجم اجازه می‌دهد با به‌دست آوردن دسترسی غیرمُجاز، دستگاه قربانی را تحت کنترل خود بگیرد و اطلاعات حساس، اعتباری و بانکی کاربر را بدزدد، در نتیجه هکر اجازه پیدا می‌کند تا از هویت قربانی برای انجام تراکنش‌های بانکی سؤاستفاده کند.

- **آگهی‌افزارها یا تبلیغ‌افزارها**[۱۶]

یکی از ساده‌ترین راه‌ها، تبلیغات است. همان‌طور که بسیاری از وِب‌سایت‌ها با نمایش تبلیغات، درآمد کسب می‌کنند، بدافزارها نیز با نمایش تبلیغات، می‌توانند مُجرمان سایبری را به درآمدزایی برسانند. آنها از تبلیغ‌افزارها، نرم‌افزارهایی که توسط برخی از برنامه‌نویسان برای ایجاد درآمد و جمع آوری داده‌ها بدون اطلاع یا رضایت قربانی نوشته شده‌اند، استفاده می‌کنند. تبلیغ‌افزارها، به‌طور خودکار آگهی‌های تبلیغاتی ناخواسته را

[14] Ransomware (e.g. WannaCry)
[15] Banking Trojans (e.g. Emotet)
[16] Adware (Ad-ware به سوی افزارها)

بدون اجازه کاربر دانلود و نمایش می‌دهند، که می‌توانند سرعت رایانه یا اینترنت شما را کم کرده یا تمرکز شما را به هم بزنند و وقت شما را تلف کنند. اینها جزء کم خطرترین و پرسودترین بدافزارهایی هستند که به شکل ابزارهای تبلیغاتی مزاحم، وارد رایانه قربانی شده و آن‌را آلوده می‌کنند اما به سختی از روی سیستم پاک می‌شوند. برخی از ابزارهای تبلیغاتی مزاحم ممکن است کاربران را فریب دهند تا بدافزاری را به عنوان نرم‌افزاری مفید دانلود، یا از وِب‌سایت جعلی و مُخربی بازدید کنند.

- **جاسوس‌افزارها**[17]

هکرها از نرم‌افزارهای جاسوسی برای نظارت بر تمام فعالیت‌های شما استفاده می‌کنند. جاسوس‌افزارها می‌توانند ضربه دکمه‌های صفحه‌کلید شما را ضبط کنند، از صفحه نمایش عکس بگیرند، وِب‌کم شما را مشاهده کنند، بر سایت‌هایی که بازدید می‌کنید نظارت کنند، و برنامه‌ها و فایل‌هایی را که روی رایانه اجرا می‌کنید، ببینند.

هنگامی که کاربر نرم‌افزارهای رایگان یا فایل‌های به ظاهر بی‌ضرر را از سایت‌های نامعتبر (دانلود و) نصب می‌کند، یا روی ابزارهای تبلیغاتی مزاحم (Adware-ها) کِلیک می‌کند، ممکن است رایانه او به‌طور ناخواسته به بدافزار جاسوس‌افزار آلوده شود.

- **کی‌لاگرها**[18]

دکمه‌نگار، ضبط‌کننده‌کلید یا کی‌لاگر، ابزاری مبتنی بر سخت‌افزار یا نرم‌افزار است که برای ردیابی یا ضبط دکمه‌های زده‌شده از روی صفحه‌کلید استفاده می‌شود. این‌کار باید به‌صورت مخفیانه انجام شود تا کاربر مطلع نشود که تحریرهای او ضبط می‌شود، و هکر هم این اجازه را داشته باشد تا پنهانی داده‌های محرمانه مانند گذرواژه‌ها، اطلاعات بانکی و کارت اعتباری را بدون اطلاع قربانی جمع آوری کند.

برای دور زدن این بدافزار یا ممانعت از این‌کار می‌توانید از صفحه‌کلیدهای مَجازی استفاده کنید. اگر وِب‌سایتی این قابلیت را در اختیار شما نمی‌گذارد و یا اینکه مجبور به

[17] Spyware (e.g. FinSpy (aka FinFisher))
[18] Keylogger

استفاده از اینترنت در کافی‌نِت‌ها هستید، برای جلوگیری از سرقت نام و گذرواژه‌هایتان قبل یا بعد آن، یا حتی به ازای هر حرفی که در فیلد کاربر یا گذرواژه وارد می‌کنید، روی قسمت دیگری از صفحه‌نمایش کِلیک کنید (تا تمرکز از روی جعبه متن برداشته شود)، سپس تعدادی دکمه را به‌صورت تصادفی فشار دهید. با انجام این روش ساده، تعداد زیادی حروف تصادفی به همراه اطلاعات اصلی در فایل کی‌لاگر ذخیره خواهند شد. گرچه اطلاعات حیاتی و حساس شما نیز در بین این حروف قرار دارد، اما کشف آنها به‌علت درهم‌ریختگی بسیار مشکل است. البته این روش نمی‌تواند مانع از کی‌لاگرهایی شود که در سطوح بالاتر فعالیت می‌کنند، یا به‌طور مستقیم مقادیر داخل فیلدها را می‌خوانند.

- **بدافزار شماره‌گیر**[۱۹]

در گذشته، بدافزاری به نام شماره‌گیر یا تماس‌گیرنده سعی می‌کرد رایانه‌هایی را که از مودم برای اتصال به اینترنت استفاده می‌کردند آلوده کند. به این شکل که با تغییر پیکربندی مودم، شماره تماس داده‌شده توسط ISP[۲۰] (فراهم‌کننده خدمات اینترنت) را به‌جای شارژ با تعرفه‌های محلی، آن‌را با تلفنی که با نرخ‌های بین‌المللی محاسبه می‌شوند، تغییر می‌داد. یا برای انتقال داده‌های دزدیده شده، به هزینه شما با هکر تماس می‌گرفت.

سایر بدافزارها

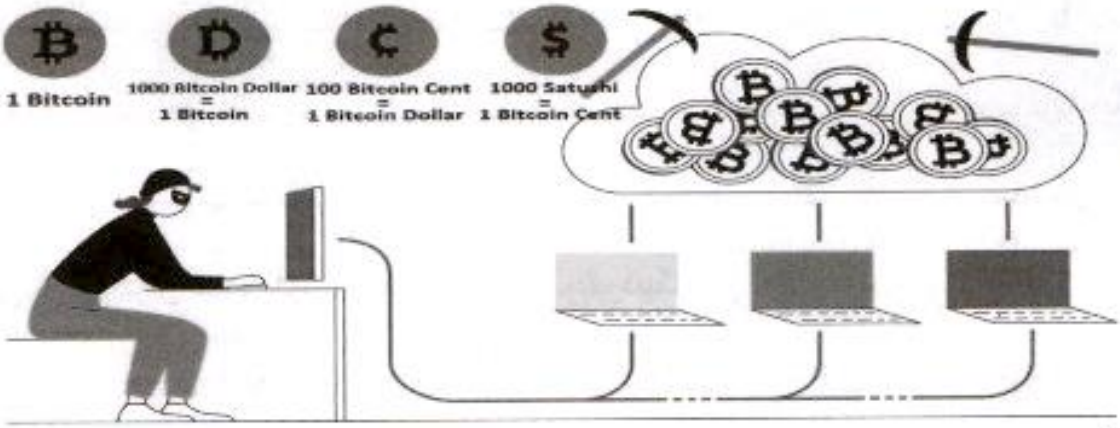
- **هراس‌افزارها**[۲۱]

اغلب ساده‌تر است قربانی را با نشر اکاذیب[۲۲] مضطرب کنید که کاری را برای شما انجام دهد تا اینکه نرم‌افزاری بنویسید که بتواند آن کارهای مُخرب را به‌صورت خودکار و بدون اطلاع وی به انجام برساند. هراس‌افزارها (ترس‌افزارها) بدافزار نیستند و کُد مُخربی برای اجرا ندارند اما از ترفندهای مهندسی اجتماعی برای التهاب آفرینی یا ترساندن کاربران و ترغیب آنها به انجام برخی کارها، سؤاستفاده می‌کنند.

[19] Dialler Malware
[20] ISP (Internet Service Provider)
[21] Scarewares
[22] Hoaxes (هشدارهای دروغین)

- **رمزارز رُبایی**[۲۳]

نوعی بدافزار که برای سرقت منابع سخت‌افزاری طراحی شده است و هکرها از راه وِب‌سایت‌ها یا لینک‌های آلوده آن‌را به رایانه قربانیان نفوذ داده و با نصب نرم‌افزارهای کاوش‌گر یا استخراج رمزارز[۲۴] کار طاقت‌فرسای معدن‌کاوی را بین هزاران دستگاه



آلوده توزیع می‌کنند[۲۵]، و چون استخراج رمزارز (یا رمزپول) به فناوری زنجیره بلوک[۲۶] و اجرای معادلات پیچیده ریاضی نیاز دارد تنها از یک بخشی از قدرت پردازشی (CPU) هر سیستم برای استخراج بیت‌کوین یا اَلت‌کوین‌های[۲۷] خود بهره‌کِشی می‌کنند تا به‌راحتی کشف نشوند و پنهان بمانند. با این‌حال، ممکن است سیستم کُند و به‌علت مصرف فراوان برق، دستگاه داغ شود و فن خنک‌کننده با سرعت بالاتری کار کند، که در مورد لپ‌تاپ یا گوشی‌های هوشمند باتری آنها سریع‌تر خالی می‌شود. اگر قربانی این تهدید را به سرعت شناسایی و از میان نبرد، با قبوض برق قابل توجهی مواجه خواهد شد.

- **نرم‌افزار امنیتی جعلی و خائن یا Rogue** (نوعی هراس‌افزار و باج‌افزار)

این برنامه به ظاهر امنیتی، وانمود می‌کند پاپ‌آپ[۲۸] قانونی است اما خائن بوده و کاربر را فریب می‌دهد که سیستم مشکل امنیتی دارد. برای مثال، به ویروس آلوده است و به‌جای از میان بردن بدافزار، برنامه ضدویروس نصب شده واقعی را خاموش می‌کند[۲۹]. بنابراین برای افزایش امنیت از برنامه‌های مطمئن، معتبر و قانونی استفاده کنید.

[23] Cryptojacking
[24] CryptoMiners (Cryptocurrency Mining)
[25] e.g. CoinHive: web-based & javascript
[26] BlockChains
[۲۷] به همه‌ی رمزارزها به جز بیت‌کوین، AltCoin (Alternative Coin) می‌گویند
[28] Pop-up windows (پنجره‌های بازشونده)
[29] SpySheriff (its clones, such as Nava Shield)

۲.۲ روش‌های مقابله و محافظت

بدافزارها پس از نفوذ به سیستم قربانی، برای کاهش احتمال تشخیص یا پاک‌سازی، از هر ترفندی استفاده می‌کنند تا خود را استتار کرده و در سیستم قربانی مخفی بمانند. از این‌رو راهبردهای دفاعی در برابر بدافزارها، بسته به نوع بدافزار متفاوت است. اما با نصب برنامه‌های ضدبدافزار/ضدویروس[۳۰] که بسیار هم مهم هستند، تشخیص آلوده بودن رایانه، کار سختی نیست. آنها با پایش سیستم، بدافزارهای مختلف را شناسایی و از میان می‌برند.

آشنایی با نرم‌افزار ضدبدافزار/ ضدویروس و محدودیت‌های آن

نرم‌افزارهای ضدویروس، برای تشخیص آلودگی از فنون مختلف زیر استفاده می‌کنند:

۱- تشخیص مبتنی بر امضاء[۳۱]:
برنامه‌های ضدبدافزار، کل سیستم را اسکن و پرونده‌ها را بررسی و امضای دیجیتالی ({83EB 0274 EB0E ...}) آنها را شناسایی، و آن‌را با امضای بدافزارهای شناخته‌شده که در بانک اطلاعاتی خود دارند، مقایسه می‌کنند تا بتوانند برنامه‌های آلوده را بیابند.

۲- تشخیص مبتنی بر ناهنجاری[۳۲]:
در این شیوه[۳۳] سیستم برای هر نوع رفتارغیرعادی تحت نظر قرار می‌گیرد. هر نوع تغییر غیرمنتظره پرونده‌ها، یا فعالیت غیرمعمول شبکه و رفتار نادرست سیستم، ممکن است نشان دهنده نوع جدیدی از ویروس باشد. این فن را به عنوان بررسی اکتشافی[۳۴] می‌شناسند. ترفند دیگر، تشخیص جعبه‌شنی[۳۵] است، برنامه مشکوک به آلودگی را در محیطی ایزوله و مَجازی اجرا می‌کنند تا نوع اقداماتی که انجام می‌دهد، ردیابی کنند. بعد، براساس نتایج به‌دست آمده مشخص می‌کنند که آیا برنامه مُخرب است یا خیر.

بدافزارها نیز برای زندگی، نیازمند مکانی هستند. حال برنامه‌ها و یا پرونده‌هایی که بدون اطلاع و مُجوز شما تغییر می‌کنند، ممکن است که آلوده شده باشند. بهترین شیوه

[30] AntiVirus/AntiMalware
[31] Signature-based detection
[32] Anomaly detection
[33] برای حملات ناشناخته
[34] Heuristic checking
[35] Sandbox detection

تشخیص تغییر[۳۶]، استفاده از هَشینگ[۳۷] است روشی که برای بررسی یک‌پارچگی داده به کار می‌رود. برای تهیه مقدار هَش[۳۸] از پرونده‌ها، می‌توان از برنامه‌های درهم‌ساز[۳۹] استفاده کرد و آنها را در مکانی امن نگه‌داری نمود. سپس به‌طور منظم در فواصل زمانی مشخص مقادیر جدید هَش را محاسبه و آنها را باهم مقایسه کرد. در صورت تغییر، شاید آلوده شده‌اند. با این روش بدافزارهای ناشناخته را هم می‌توانید کشف کنید.

نرم‌افزار ضدویروس برای عملکرد خود به فهرستی به‌روز شده از جدیدترین ویروس‌ها و سایر بدافزارها نیاز دارد تا بتواند در محافظت از سیستم‌ها مؤثر باشد. زیرا بدون انجام این‌کار، نرم‌افزار ممکن است قادر به شناسایی ویروس‌های جدید و توسعه‌یافته نباشد. بسته به میزان به‌روز رسانی نرم‌افزار، قابلیت‌های نرم‌افزارهای مختلف ضدویروس متفاوت است. همچنین نصب دیواره‌آتش (فایروال[۴۰]) برای ایمن‌سازی شبکه‌ها از نفوذ، اِعمال وصله‌های[۴۱] منظم برای کاهش حملات روز-صفر[۴۲]، داشتن برنامه برای پشتیبان‌گیری منظم و ایزوله کردن سیستم‌های آلوده، به‌روز نگه داشتن مرورگرهای وِب، افزونه‌ها[۴۳]، برنامه‌ها و سیستم عامل‌ها ضروری است زیرا اکثر وصله‌ها یا به‌روز رسانی‌ها، حفره‌های نفوذ و نقض‌های امنیتی شناخته شده برنامه‌ها را رفع کرده‌اند و از آنجا به بعد است که می‌توانند سیستم شما را در برابر تهدیدات ویروس‌های جدید، توسعه داده شده و پیچیده، محافظت کنند.

[36] Change detection
[37] Hashing
[38] Hash value
[39] IgorWare Hasher, HashCheck/Tools, ...
[40] Firewall (فصل ۳ را ببینید)
[41] Patches
[42] Zero-day attacks
[43] Plug-ins

محدودیت‌ها:

- **امکانات نرم‌افزار ضدویروس**

با نصب نرم‌افزارهای ضدویروس یک لایه امنیتی به سیستم دفاعی خود اضافه می‌کنید. بنابراین باید به گونه‌ای پیکربندی و تنظیم شوند که درایوها، پوشه‌ها، پرونده‌ها، برنامه‌ها، درگاه‌های USB و حافظه‌های رَم، را به‌صورت دوره‌ای، یا در زمان‌های مشخص و به فراخور نوع سیستم و حساسیت‌های آن، به‌صورت خودکار مورد پایش قرار بگیرند. همچنین باید تمامی اِیمیل‌ها به‌ویژه ضمائم آنها برای وجود کُدهای مُخرب بررسی شوند. هنگامی که نرم‌افزار ضدویروس با یک برنامه یا پرونده آلوده مواجه می‌شود، به‌طور کلی سه گزینه در اختیار می‌گذارد: تمیز کردن، قرنطینه کردن[۴۴]، یا حذف کردن.

عمل قرنطینه، تلاش می‌کند تا موارد مشکوک به آلودگی را به مکان امنی که توسط نرم‌افزار ضدویروس مدیریت می‌شود، منتقل کند، تا خود کاربر در خصوص آنها، تصمیمات مناسب و مقتضی را اتخاذ نماید. اما بهتر است که بدافزارها به محض کشف، به‌طور کامل پاک و ریشه‌کن شوند، و آثار آن نیز از کلیه مکان‌های محتمل (مثل NFS[۴۵]، FAT[۴۶]، Boot Sector، فایل‌های رجیستری) حذف شود.

نرم‌افزارهای مختلف ضدویروس (آنتی‌ویروس)، قابلیت‌ها و ویژگی‌های متفاوتی دارند، و هیچ ضدبدافزاری امکان تشخیص همه‌ی برنامه‌های مُخرب را ندارد. از ساده‌ترین آنها که برای کشف و پاک کردن یک نوع خاصی از بدافزارها طراحی شده‌اند تا آنهایی که شما را در برابر انواع پیچیده‌تر محافظت می‌کنند، امکان تشخیص همه‌ی برنامه‌های مُخرب را ندارند. با این‌حال، برنامه‌هایی وجود دارند[۴۷] که می‌توان یک لایه‌ی حفاظتی دیگری به سیستم اضافه نمود. در انتخاب و نصب نرم‌افزارهای ضدویروس دقت کافی را داشته باشید زیرا نصب چند برنامه ضدبدافزار در یک سیستم ممکن است

[44] Quarantine Files
[45] NFS (Network File System)
[46] FAT (File Allocation Table)
[47] e.g. AppLocker

علاوه بر کاهش کارآیی باعث بروز ناسازگاری شوند. اگر برنامه ضدبدافزاری را نصب نکرده‌اید یا می‌خواهید از قابلیت‌های متنوع آنتی‌ویروس‌های مختلف استفاده نمایید، می‌توانید از منابع برخط و معتبر در اینترنت کمک بگیرید[۴۸]. همچنین می‌توانید با استفاده از برخی سایت‌های سیستم عامل‌ها، ضدویروس‌ها، مرورگرها، و ...، حملات و آلودگی‌های بدافزاری بر روی سیستم خود را کشف و سپس آنها را از میان ببرید.

- **سؤاستفاده یا بهره‌کِشی روز-صفر[۴۹]**

آسیب‌پذیری روز-صفر[۵۰] به یک نقص امنیتی ناشناخته، ضعف نامشخص یا اشکال اصلاح نشده در نرم‌افزار، سفت‌افزار[۵۱] یا سخت‌افزار گفته می‌شود که ممکن است محققان پیش از این، آن آسیب‌پذیری را کشف و فاش کرده باشند، یا حتی شرکت‌های توسعه‌دهنده نیز از قبل، از این مشکل امنیتی آگاه شده باشند، اما هنوز وصله امنیتی یا به‌روز رسانی رسمی که آن‌را رفع کرده باشد، منتشر نشده است. هکرها اغلب این نوع آسیب‌پذیری‌ها را قبل از طراحان و توسعه‌دهندگان، شناسایی و سعی می‌کنند پیش از گزارش و انتشار عمومی آن برای اصلاحیه و ترمیم حفره امنیتی، از این اِکسپلویت ناشناخته برای حملات روز-صفر و یا سایر اقدامات مُخرب سؤاستفاده کنند.

کُدی که اغلب برای سؤاستفاده از آسیب‌پذیری نوشته می‌شود، اِکسپلویت[۵۲] می‌نامند و بهره‌کِشی روز-صفر، نوعی حمله به سیستم است که از آسیب‌پذیری روز-صفر بهره می‌برد و می‌تواند بر سازمان‌هایی که برنامه‌ها را به‌روز رسانی یا وصله نمی‌کنند تاثیر سؤ بگذارد.

- **آسیب‌پذیری‌های ذاتی**

برنامه‌های ضدویروس نیز با محدودیت مواجه‌اند، زیرا نمی‌توانند جلوی سؤاستفاده‌هایی که به نقص‌های امنیتی یا به آسیب‌پذیری‌های ذاتی سیستم عامل حمله می‌کنند، را بگیرند.

---

[48] www.virustotal.com
[49] Zero-day exploit
[50] Zero-day vulnerability

[۵۱] Firmware، میکروکُدی برای کنترل بهینه‌تر سخت‌افزار که شبیه سیستم عامل دستگاه عمل می‌کند
[52] Exploit

به‌روز رسانی نرم‌افزار ضدویروس

نرم‌افزار ضدویروس برای شناسایی تهدیدها از فایل تعریف ویروس که به پایگاه داده ویروس‌ها معروف است، استفاده می‌کند. به‌روز رسانی این فایل[۵۳] بسیار مهم است زیرا برنامه را قادر می‌سازد تا ویروس‌های جدیدتر و پیچیده‌تر را شناسایی کند. بنابراین عدم به‌روز رسانی به موقع برنامه‌ها، بسیار خطرناک است زیرا کاربران **تصور نکنند** که تنها نصب برنامه ضدویروس کفایت کرده و او می‌تواند آنها را در مقابل هر نوع حملاتی محافظت کند، غافل از اینکه در واقع در معرض تمام حملات جدید قرار دارند.

برای مثال، در زیر یک نمونه کار با برنامه ضدویروس مایکروسافت آورده شده است.

Using an Anti-Virus Software

Software: Microsoft Security Essentials
Scanning: Home tab> Quick Scan / Full Scan
Scanning Specific Drives: Home tab> Custom
Scheduling Scans: Settings tab> Scheduled scan
Updating Virus Definition: Update tab> Update

کارگاه آموزشی

۱- از ابزار virustotal استفاده کنید تا از ایمن بودن پرونده قبل از دانلود مطمئن شوید.

۲- با نرم‌افزار Applocker تمرین کنید.

۳- با یکی از برنامه‌های ضدویروس ص ۵۴ که به آن دسترسی دارید، کار کنید.

[۵۳] بانک اطلاعاتی امضاء دیجیتال

فصل ۳

امنیت شبکه

شبکه رایانه‌ای، گروهی از دو یا چند سیستم رایانه‌ای است که توسط کانال‌های ارتباطی به یک‌دیگر متصل شده‌اند تا امکان اشتراک‌گذاری منابع و اطلاعات را فراهم کنند. دستگاه‌های موجود (مانند رایانه‌ها، وسایل ذخیره‌ساز، چاپگرها، مسیریاب‌ها[۱]، نقاط دسترسی[۲] و ...) در شبکه را گره[۳] می‌نامند. گره‌ها را می‌توان با استفاده از انواع مختلفی از رسانه‌های اتصال، یا به‌صورت سیمی و فیبر نوری، یا به‌صورت بی‌سیم با امواج الکترومغناطیس مانند امواج رادیویی (برای مثال وای‌مَکس (WiMAX[۴])، وای-فای (Wi-Fi[۵]))، و یا امواج نوری (مانند مادون قرمز[۶]) به هم متصل کرد.

برای ارتباط بین گره‌ها و رسانه‌های اتصال، به واسط‌های سخت‌افزاری به نام مبدل‌ها[۷] نیاز می‌باشد. برای محیط‌های سیمی از کارت شبکه، و برای بی‌سیم از مبدل‌های مخصوص بی‌سیم (به نام روترهای وای-فای) استفاده می‌کنند. و در آخر، برای نظام‌مند نمودن اتصال و تبادل داده‌ها بین دستگاه‌های فوق باید از قوانین، الگوریتم‌ها و استانداردهایی برای کنترل، مدیریت و سازمان‌دهی ترافیک شبکه، موسوم به **پروتکل‌های ارتباطی**[۸] بهره بگیریم.

---

[1] Router, Network Layer (OSI layer 2)
[2] AP (Access Point)
[3] Node
[4] WiMAX (Worldwide Interoperability for Microwave Access)
[5] Wi-Fi (Wireless Fidelity)
[6] InfraRed
[7] Adapters
[8] Ethernet (IEEE 802.3), https, FTP, SSH, ...

۱.۳ انواع شبکه‌های رایانه‌ای

شبکه‌ها برحسب معماری، توپولوژی، اندازه و فواصل فیزیکی یا محدوده جغرافیایی و یا بسته به اینکه چه اشخاصی از آنها استفاده می‌کنند، به انواع مختلفی طبقه‌بندی می‌شوند.

- **LAN[۹] (شبکه محلی)**

شبکه محلی کوچکترین نوع شبکه است که منطقه جغرافیایی محدودی مانند یک ساختمان یا یک سازمان را پوشش می‌دهد. هنگامی که کاربران رایانه‌های خود را به شبکه LAN متصل می‌کنند، باید نام کاربری و رمز عبور خود را وارد کنند. پس از احراز هویت، بسته به نوع مُجوزهای اختصاص داده شده به حساب آنها، می‌توانند به خدمات موجود در شبکه و منابع مشترک (مانند اتصال به اینترنت، درایوهای شبکه، چاپگرها و همچنین رایانه‌های دیگر کاربران) دسترسی داشته باشند. رایج‌ترین قرارداد ارتباطی به کار رفته در LAN، فناوری اِترنت[۱۰] است که تحت استاندارد IEEE[11] 802.3 می‌باشد. این فناوری برای مبادله داده، از ۸ رشته سیم مسی عایق‌شده تلفن معمولی استفاده می‌کند که به‌خاطر کاهش تداخل و القاهای الکترومغناطیسی، دوبه‌دو به هم تابیده شده‌اند.

- **VLAN[۱۲] (شبکه محلی مَجازی)**

یک شبکه همپوشانی منطقی است که اجازه می‌دهد تا چندین شبکه مَجازی بر روی یک شبکه فیزیکی منفرد (اِترنت، بی‌سیم و ...) به‌صورت منطقی[۱۳] گروه‌بندی شوند و ترافیک هر گروه را به مانند یک شبکه محلی مجزا و مستقل مدیریت می‌کند.

- **WLAN[۱۴] (شبکه محلی بی‌سیم)**

در مکان‌هایی که ایجاد شبکه هزینه‌بر یا غیرممکن باشد، از شبکه‌های بی‌سیم که در آنها داده‌ها توسط امواج الکترومغناطیسی منتقل می‌شوند، استفاده می‌کنیم.

---

[9] LAN (Local Area Network)
[10] Ethernet
[11] IEEE (Institute of Electrical and Electronics Engineers)
[12] VLAN (Virtual LAN)
[13] At the Data Link Layer (OSI layer 2)
[14] WLAN (Wireless LAN)

برای شبکه‌سازی بی‌سیم با امواج رادیویی می‌توان به این موارد اشاره نمود:

- شبکه‌های بی‌سیم مجاور[15] (بسیار نزدیک هم) مانند RFID یا NFC،
- شبکه‌های بی‌سیم شخصی[16] مثل بلوتوث[17]،
- شبکه‌های بی‌سیم محلی مانند وای-فای، در این شبکه، کاربران (موبایل یا لپ‌تاپ) اجازه دارند در یک منطقه محدود مانند خانه، اداره، مدرسه، دانشگاه، فرودگاه، فروشگاه و ...، با استفاده از امواج رادیویی به یک‌دیگر و اینترنت متصل شوند. در شبکه‌های بی‌سیم برای تبادل داده‌ها در یک محدوده مشخص و همچنین برای اتصال به اینترنت از تجهیزات نقطه دسترسی بی‌سیم (یا WAP[18]) استفاده می‌کنیم،
- شبکه‌های بی‌سیم شهری[19] برای مثال وای-مَکس،
- شبکه‌های بی‌سیم گسترده[20] مانند شبکه‌های سلولی تلفن همراه[21]،
- شبکه بی‌سیم نوری یا Li-Fi، وقتی دستگاه‌های زیادی روی یک فرکانس به تبادل اطلاعات می‌پردازند، سرعت و کارآیی وای-فای به شدت افت می‌کند. برای حل این مشکل از نور مرئی یا امواج مادون قرمز بهره می‌گیرند. این شبکه‌ها سرعت و پهنای باند بالایی دارند، و با افزایش تعداد تجهیزات متصل به شبکه کاهش نمی‌یابد و از امنیت بالاتری هم نسبت به وای-فای برخوردارند. اما برای برقراری ارتباط، باید AP شبکه و دستگاه‌های دریافت کننده، در دید مستقیم هم باشند.

- **WAN[22] (شبکه گسترده)**

شبکه گسترده (WAN)، نسبت به LAN می‌تواند منطقه جغرافیایی وسیعی‌تری مانند، یک شهر، کشور یا چند قاره را پوشش دهد. بسیاری از سازمان‌ها و شرکت‌های نوین که دفاتر آنها در نقاط مختلف شهرهای بزرگ یا سطح کشور پراکنده‌اند و یا در سراسر جهان نمایندگی دارند، می‌توانند شبکه‌های محلی خود را با استفاده از مسیریاب‌ها و

[15] Adjacent Wireless Network
[16] PAN (Personal Area Network)
[17] Bluetooth (IEEE 802.15)
[18] WAP (Wireless Access Point)
[19] WMAN (Wireless Metropolitan Area Network)
[20] WWAN (Wireless WAN)
[21] Cellular: 3G/4G/5G/6G, GSM, LTE, ...
[22] WAN (Wide Area Network)

لینک‌های ارتباطی عمومی مانند خطوط مخابراتی یا امواج رادیویی به هم متصل کنند، و یک شبکه گسترده سازمانی تشکیل بدهند. کارکنان آنها هم که در مکان‌های مختلف کار می‌کنند می‌توانند به اطلاعات و سامانه‌های یکسانی دسترسی داشته باشند، و بر خلاف LAN، مجبور نیستند که سخت‌افزار یا نرم‌افزاری را به اشتراک بگذارند. بزرگترین شبکه WAN موجود، **اینترنت** است.

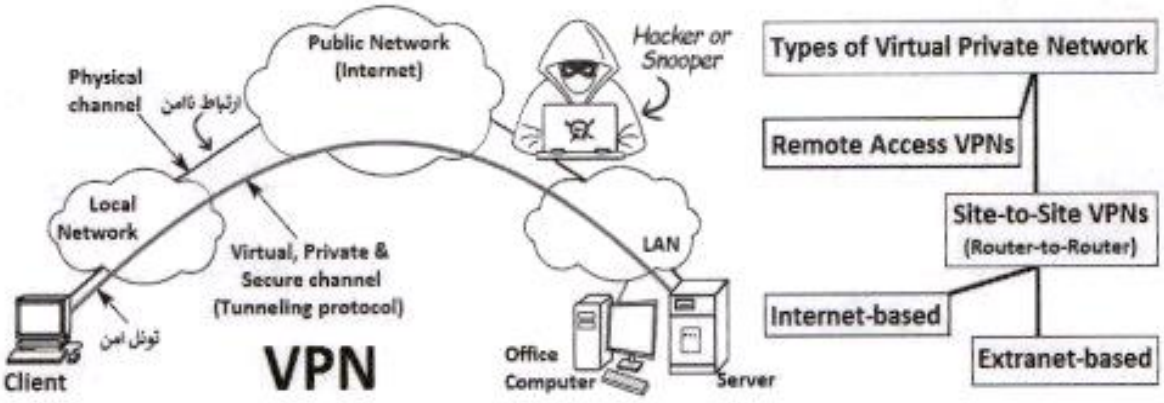
- **شبکه‌ای از شبکه‌ها**

دو یا چند شبکه یا زیرشبکه[۲۳] که با استفاده از تجهیزاتی مانند مسیریاب، به یک‌دیگر متصل می‌شوند، تشکیل شبکه‌ای از شبکه‌ها یا شبکه متصل[۲۴] را می‌دهند. بسته به اینکه چه کسانی، آن‌را مدیریت می‌کنند و اینکه چه افرادی در این شبکه عضو هستند، می‌توان سه نوع «شبکه متصل» داشت:

- شبکه داخلی یا اینترانت[۲۵]، اینترانت یا وِب‌سایت داخلی، به شبکه‌های محلی هر شرکت یا سازمانی گفته می‌شود که به‌صورت خصوصی اداره می‌شوند و تنها افراد دارای مُجوز می‌توانند به آن دسترسی داشته باشند.
- شبکه بیرونی یا اکسترانت[۲۶]، مشابه اینترانت، اکسترانت یک شبکه محلی است که دست کم یک اتصال به خارج از شبکه داشته باشد و فقط کارکنان و کسب‌وکار شرکت از خارج آن، دسترسی دارند. اما هنوز عموم مردم به آن دسترسی ندارند.
- شبکه جهانی یا اینترنت[۲۷]، به شبکه ویژه‌ای از شبکه‌ها که حاصل اتصال شبکه‌های دولتی، دانشگاهی، شرکت‌های عمومی و خصوصی در سراسر دنیا است، **شبکه اینترنت** می‌گویند. این شبکه بر اساس طرح آرپانِت ARPANET[۲۸] ایجاد شده و پروتکل آن بر اساس مدل سرویس‌گیرنده/سرویس‌دهنده[۲۹] می‌باشد و منزلگاه اصلی

[23] Subnet
[24] Internetwork
[25] Intranet
[26] Extranet
[27] Internet
[28] By the U.S Department of Defense
[29] Client/Server

وِب WWW[۳۰] است. شبکه‌های داخلی یا بیرونی که به شبکه اینترنت متصل می‌شوند، باید در مقابل دسترسی‌های غیرمُجاز از سوی شبکه ناامن اینترنت محافظت شوند.



- **VPN[۳۱] (شبکه خصوصی مَجازی)**

هر شرکتی برای خود، یک شبکه سازمانی دارد که به‌صورت اختصاصی اداره می‌شود. شبکه خصوصی مَجازی (VPN) به کاربران مُجاز اجازه می‌دهد تا با استفاده از بستر شبکه‌های عمومی و ناامن مانند اینترنت، به شبکه سازمانی خود به‌صورت امن متصل شوند. کاربران می‌توانند از راه دور و با یک ارتباط رمزگذاری شده به منابع شبکه، چاپگرها، سایت‌های اینترانت، پایگاه‌های داده و سایر خدمات قابل ارائه در سازمان خود، که به اشتراک گذاشته شده‌اند، به‌صورت ایمن دسترسی داشته باشند. این روش، به کاربران اجازه می‌دهد تا داده‌ها را به شکل امن، ارسال و دریافت کنند. گویی که به‌طور مستقیم و اختصاصی به شبکه محلی (LAN) سازمان متصل هستند. VPN برای امنیت بیشتر، از ترافیک رمزگذاری شده و پروتکل‌های تونل‌زنی[۳۲] برای ایجاد یک اتصال نقطه به نقطه مَجازی بین کاربر و شبکه خصوصی استفاده می‌کند.

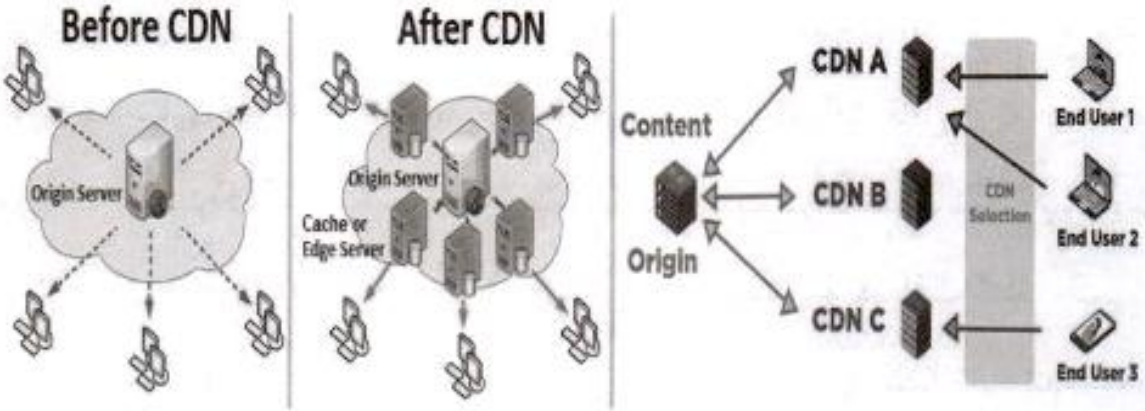
کشورها برای حفظ سلامت روانی جامعه و برای پیشگیری از دسترسی کودکان به سایت‌های غیراخلاقی به شیوه‌های سخت‌افزاری و نرم‌افزاری اقدام به غربال‌سازی اینترنت یا فیلترینگ می‌کنند. اما برخی از شرکت‌ها برای دور زدن آن، فناوریی از VPN

[30] WWW (World Wide Web) (تار جهان‌گستر)
[31] VPN (Virtual Private Network)
[32] Tunneling Protocols: IPSec, L2TP, GRE, SSL, MPLS, OpenVPN, WireGuard, ...

استفاده می‌کنند که به فیلترشکن معروف هستند. VPN-هایی که به عنوان فیلترشکن عمل می‌کنند با استفاده از تونل‌زنی، فیلترینگ مخابرات و ISP را دور می‌زنند. اگر سِرور وی‌پی‌اِن به کنترل یک هکر درآید، به تمام اطلاعات هویتی و دیگر داده‌های حساس مثل رمزهای عبور، اطلاعات بانکی و ...، دسترسی پیدا کرده و آنها را خواهد دزدید. بنابراین هوشیار باشید وقتی از VPN-های غیرسازمانی یا فیلترشکن استفاده می‌کنید هرگز به سایت‌های خرید-فروش، اِیمیل و به‌ویژه بانک خود وارد نشوید.

- **شبکه‌های تحویل محتوا** یا CDN[۳۳]

نوعی شبکه از سیستم‌های توزیع‌شده است که سازمان‌ها برای پایداری و پیوستگی خدمات اینترنتی و افزایش سرعت دستیابی، محتوای وِب‌سایت‌های خود را به‌جای میزبانی در یک مرکز داده منفرد با سِرورهای قوی، در مراکز داده‌ی مناطق مختلف جغرافیایی با سِرورهای رده متوسط پخش می‌کنند. هدف از ایجاد این شبکه‌ها، در وهله



اول برای مقابله با حملات DoS و DDoS بوده که به منظور پایداری و افزایش میزان دسترس‌پذیری و بهبود عملکرد شبکه صورت می‌پذیرد، و دلیل بعد اینکه کاربران بتوانند به نزدیک‌ترین سِرور منطقه جغرافیایی خود وصل شوند تا با سرعت بیشتری نسبت به روش سنتی، وِب‌سایت‌ها را بارگیری کنند. با وجود مزایای زیاد CDN، پیاده‌سازی چنین شبکه‌ای، دانش و پیچیدگی‌های خاص خود را دارد.

[33] CDN (Content Delivery Networks)

مخاطرات و پیامدهای امنیتی اتصال به شبکه

دستگاه‌ها می‌توانند به یکی از دو روش:

۱- اتصالات کابلی شبکه و ۲- نقاط دسترسی بی‌سیم (WAP)

به شبکه‌ها وصل شوند. به این ترتیب هر فردی می‌تواند یک دستگاه ناامن را به یک شبکه ناامن متصل کند، و به منابع و داده‌های به اشتراک گذاشته شده، دسترسی پیدا کند. این‌کار، شبکه و تمام دستگاه‌هایی که به آن متصل هستند، از جمله سِرورها را، به خطر می‌اندازد. پیامدهای امنیتی که هنگام اتصال به شبکه ممکن است اتفاق بیفتند، عبارتند از:

- **آلودگی به بدافزار**

  اتصال دستگاه‌ها به شبکه‌ها، یا وصل کردن فلش‌مِموری به یک دستگاه متصل به شبکه، به بدافزارها و ویروس‌های موجود در یک دستگاه محافظت‌نشده اجازه می‌دهد تا به‌راحتی از راه شبکه ناامن به دستگاه‌های دیگر سرایت، و کل شبکه را آلوده کنند.

- **ایجاد دسترسی غیرمُجاز به داده‌ها**

  اگر یک مزاحم بتواند به شبکه دسترسی پیدا کند، می‌تواند داده‌های محافظت نشده را بخواند و به‌راحتی اسرار تجاری و داده‌های محرمانه یا حساس شرکت را به خطر بیندازد. برای مثال، می‌تواند مالکیت معنوی اعضای سازمان را در معرض دید عموم قرار دهد.

- **نقض حریم خصوصی**

  اتصال دستگاه شما به یک شبکه ممکن است این امکان را ایجاد کند که سایر کاربران شبکه، بتوانند به اطلاعات ما در دستگاه شما دسترسی داشته باشند.

اما اجرای صحیح خط‌مشی‌های امنیت شبکه باعث کاهش یا حذف این تهدیدها می‌شود.

نقش و وظایف مدیر شبکه

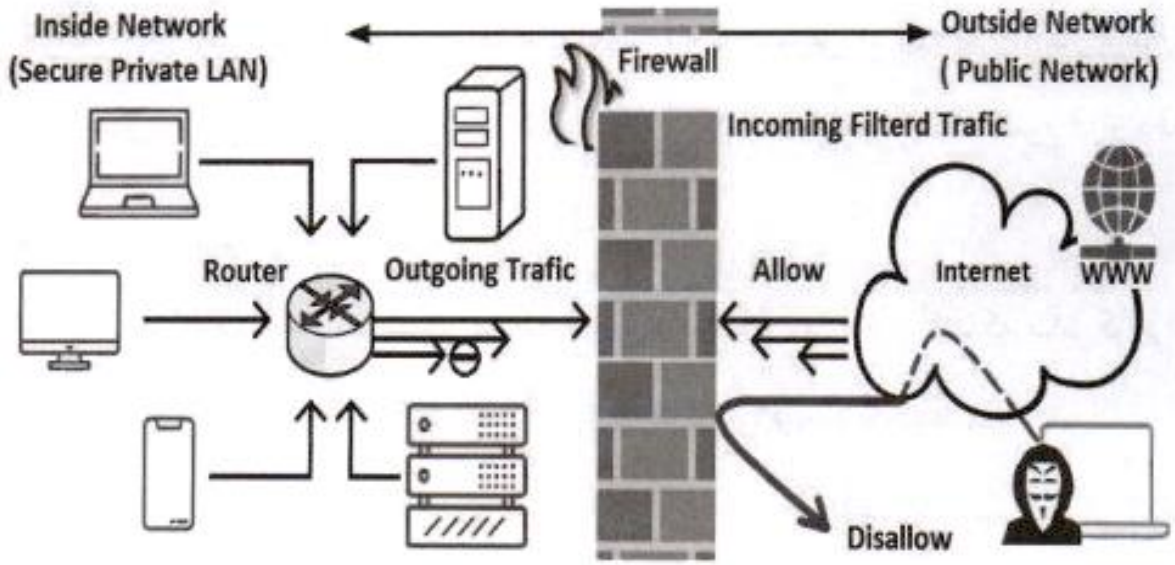
مدیر شبکه فردی است که مسئول نگه‌داری سخت‌افزار، نرم‌افزار و سایر تجهیزاتی است که یک شبکه رایانه‌ای را تشکیل می‌دهد. این، به‌طور معمول شامل استقرار، پیکربندی،

نگه‌داری و نظارت بر تجهیزات فعال شبکه است. یک جزء مهم از نقش مدیر شبکه به امنیت مربوط می‌شود. فعالیت‌های مرتبط با امنیت او می‌تواند مواردی از این دست باشند:

- مدیریت احراز هویت و اعطای مُجوز به حساب‌های کاربری در شبکه.
- حفظ و صیانت از دسترسی کارکنان به داده‌های مورد نیاز در شبکه و اطمینان از اینکه استفاده از شبکه در راستای سیاست‌های ICT (سازمان یا شرکت) است.
- نظارت، کنترل و نصب وصله‌ها و به‌روز رسانی‌های امنیتی مربوطه، نظارت بر ترافیک شبکه و مقابله با بدافزارهای موجود در شبکه، و حملاتی که به آن صورت می‌گیرد.

دیواره‌آتش - عملکرد و محدودیت‌ها

اولین ابزار کنترل دسترسی و سد دفاعی در شبکه که به‌صورت پیشگیرانه عمل می‌کند، حصاری است به نام **دیواره‌آتش** یا **دژبان**. دیواره‌آتش، برنامه یا یک دستگاه سخت‌افزاری است که از آن برای محافظت از شبکه در برابر هکرهایی که سعی دارند به سیستم‌ها نفوذ کنند و به داده‌های آنها دسترسی پیدا کنند، استفاده می‌شود. فایروال شبکه، اطلاعاتی را که از راه اتصال اینترنت به/از رایانه شخصی شما یا شبکه شرکت می‌رسد، فیلتر می‌کند.



فایروال‌ها مانند یک مانع و دیوار حائل بین شبکه داخلی و شبکه ناامن بیرونی (مثل اینترنت) عمل می‌کنند. هنگامی که هر ترافیکی از خارج از شبکه سعی می‌کند به شبکه

داخلی دسترسی پیدا کند، فایروال مجموعه‌ای از قوانین و معیارهای موجود را بر روی آن بررسی می‌کند، و چنانچه داده‌ای که می‌آید از منبعی غیرمُجاز باشد، آن‌را مسدود می‌کند. با اینکه فایروال‌ها از اجزای حیاتی زیرساخت امنیتی شبکه هستند، محدودیت‌هایی دارند:

- **ویروس‌ها**

همه فایروال‌ها نمی‌توانند حفاظت کاملی در برابر ویروس‌ها یا خطرات امنیتی غیرفنی (مانند مهندسی اجتماعی) برقرار کنند. همچنین قادر به جلوگیری در برابر انتقال فایل‌ها، برنامه‌ها یا نرم‌افزارهای آلوده هم نیستند.

- **حملات**

فایروال‌ها نمی‌توانند شبکه را در برابر حمله‌هایی که از آنها عبور نمی‌کنند محافظت کنند. همچنین هیچ کنترلی در برابر دسترسی بی‌سیم و سایر دسترسی‌هایی که شما در سیستم‌های خود ایجاد کرده‌اید، ندارند. برای مثال، دیواره‌آتش شاید دسترسی از اینترنت یا به آن‌را محدود کند، اما ممکن است در برابر کاربرانی که لپ‌تاپ‌ها و سایر دستگاه‌های همراه آلوده را به شبکه شرکت متصل می‌کنند، محافظتی انجام ندهد.

- **نظارت و دیده‌بانی**

سازمان‌ها و شرکت‌ها برای محافظت خود در اینترنت، اطمینان از نظارت کارآمد و دیده‌بانی کامل ترافیک شبکه از دیواره‌آتش استفاده می‌کنند، و اگر به درستی تنظیم و پیکربندی نشود، نمی‌تواند هشدارهای لازم را اطلاع دهد، یا با هشدارهای بی‌موردی که ممکن است مُخرب نباشند، حساسیت و هوشیاری را نسبت به هشدارها از میان ببرد[۳۴].

دیواره‌آتش شخصی[۳۵]

فایروال‌ها، تجهیزاتی هستند که به‌صورت سازمانی و شخصی استفاده می‌شوند. امروزه اکثر دستگاه‌های شخصی (مانند رایانه‌های شخصی، لپ‌تاپ‌ها، گوشی‌های هوشمند، ...) برای افزایش امنیت، از دیواره‌آتش شخصی که به‌صورت توکار در سیستم عامل‌ها تعبیه شده

[34] Titanic (1997 film)

[35] Personal Firewall

است، استفاده می‌کنند، که با فعال نمودن آن، موقع اتصال به اینترنت به‌خصوص توسط وای-فای عمومی در مکان‌هایی مانند هتل، دانشگاه، کتاب‌خانه، کافه، فرودگاه و غیره، از شما محافظت می‌نماید. اما از نظر قابلیت و مقیاس با فایروال‌های معمولی شبکه (که روی واسط‌های خاصی بین دو یا چند شبکه نصب می‌شوند)، متفاوت است.

با فایروال شخصی، تنها می‌توان خط‌مشی امنیتی را برای دستگاه‌های شخصی تعریف کرد، در حالی که با دیواره‌آتش معمولی، خط‌مشی را می‌توان بین رایانه‌ها و شبکه‌هایی که به‌صورت گروهی به هم متصل می‌شوند، کنترل نمود. ضروری است هر فردی که به اینترنت دسترسی دارد (به‌خصوص با وای-فای‌های عمومی)، مطمئن شود که یک دیواره‌آتش شخصی نصب و آن‌را فعال کرده است، تا بتواند از ورود ترافیک‌های غیرمُجاز ممانعت کند.

دستگاه‌های مَک، ویندوز، لینوکس و اکثر WAP-ها، دیواره‌آتش داخلی دارند، که فقط از سیستمی که روی آن نصب شده‌اند محافظت می‌کنند. با این‌حال، استفاده از فایروال‌های معتبر[۳۶]، می‌تواند امنیت دستگاه‌ها را افزایش و محافظت بهتری را فراهم کند.

۲.۳ امنیت شبکه‌های بی‌سیم

شبکه‌های بی‌سیم راهی آسان و مناسب برای اتصال به اینترنت، به‌ویژه با دستگاه‌های قابل حمل مانند تلفن‌های هوشمند، لپ‌تاپ‌ها یا تبلت‌ها می‌باشند. هنگام جستجوی شبکه‌های بی‌سیم محیط اطرافمان، برخی از اتصالات ناامن و برخی دیگر شبکه‌های ایمن هستند. شبکه‌های ناامن برای اتصال هر دستگاه به شبکه بی‌سیم، که می‌توانند دسترسی نامحدود به داده‌ها و منابع دستگاه‌های دیگر را امکان‌پذیر سازند، هیچ‌گونه احرازهویتی انجام نمی‌دهند. اما شبکه‌های امن، شبکه‌هایی هستند که با گذرواژه‌های امنیتی و رمزگذاری توسط مدیر شبکه راه‌اندازی شده‌اند و قبل از ورود به سیستم، به کلید ورودی آن نیاز دارید.

[36] Comodo, ZoneAlarm, TinyWall, ...

اتصالات بی‌سیم، محدودیت‌های شبکه فیزیکی را ندارند اما با مشکلات امنیتی مشابهی روبرو هستند، و اگر درست محافظت نشوند خطر حمله‌های شنود، آنها را تهدید خواهد کرد:

- **شنود (استراق سمع)**[۳۷] – افراد غریبه یا سایر اشخاص به داده‌های در حال مبادله شما دسترسی دارند و می‌توانند آنها را برای یافتن اطلاعات حساس یا محرمانه بخوانند.
- **ربودن شبکه**[۳۸] **(شبکه‌رُبایی)** – اگر مسیر به درستی رمزگذاری نشود، مهاجمین به‌راحتی می‌توانند ارتباطات شما با شبکه را در دست بگیرند.
- **حمله مرد میانی**[۳۹] – مهاجم بین دو طرف قرار می‌گیرد و مخفیانه ارتباطات بین آنها را که فکر می‌کنند به‌طور مستقیم و خصوصی با یک‌دیگر در ارتباط هستند، رهگیری، تغییر و دوباره بازپخش[۴۰] می‌کند.

تنظیمات امنیتی بی‌سیم

دروازه ارتباطی شبکه‌های بی‌سیم با اینترنت، مودم‌های Wi-Fi (یا WAP‌ـها) هستند و اگر به درستی تنظیم، رمزگذاری و محافظت نشوند در معرض انواع حملات شنود قرار می‌گیرند. بهترین و ساده‌ترین راه مقابله، تغییر تنظیمات پیش‌فرض مودم-روتر Wi-Fi و ایمن‌سازی آن با توجه به شیوه‌ی احرازهویت و روش رمزگذاری می‌باشد. برای ورود به صفحه تنظیمات ابتدا باید در مرورگر خود، IP مودم-روتر (192.168.1/0.1) را وارد کنید.

۱- **رمزعبور مودم-روتر**، اولین و اساسی‌ترین قدم، انتخاب یک گذرواژه مستحکم برای مودم-روتر است تا مطمئن شوید رمز عبوری که انتخاب کرده‌اید به‌راحتی توسط هکرها شکسته نمی‌شود. سایر اقدامات امنیتی از جمله تولید کلید رمزنگاری که قرار است توسط پروتکل‌های امنیتی، ترافیک شبکه را رمزگذاری کنند، به این امر بستگی دارد.

[37] Eavesdropping
[38] Network Hijacking
[39] MitM (Man-in-the-Middle)
[40] Replay

۲- **پروتکل‌های امنیتی**، رایج‌ترین پروتکل‌های امنیتی که برای اعتبارسنجی و رمزگذاری شبکه‌های وای-فای (صدور گواهی‌نامه امنیتی بین کلاینت‌ها و WAP) به کار می‌روند و در مودم-روترهای مربوطه قابل تنظیم‌اند، عبارتند از:

- **WEP**[۴۱] - این استاندارد خیلی قدیمی و آسیب‌پذیر است، و نباید استفاده شود.
- **WPA**[۴۲] - اطلاعاتی را که بین دو دستگاه متصل رد و بدل می‌شود رمزگذاری و کاربران را نیز احرازهویت می‌کند و فقط به این کاربران احراز هویت شده اجازه می‌دهد تا به شبکه‌های بی‌سیم متصل شوند و داده‌ها را با سایر دستگاه‌های موجود در آن شبکه مبادله کنند. سه نوع احراز هویت WPA وجود دارد:
  - (WPA-PSK (TKIP/AES)[۴۳])، این شیوه آسیب‌پذیر بوده و نباید استفاده شود.
  - **WPA2**، این پروتکل با گزینه WPA2 + AES همراه با غیرفعال کردن WPS[۴۴] به شما اجازه می‌دهد در شرایط بهتری، یک ارتباط وای-فای امن را تجربه کنید.
  - **WPA3**، این پروتکل آسیب‌پذیری‌های WPA2 را ترمیم و احراز هویت PSK را با پروتکل قوی‌تر و امن‌تر تبادل کلید SAE[۴۵] بهبود می‌بخشد و اتصال به WAP-ها را بدون در نظر گرفتن رمزمودم با یک کلید اختصاصی، رمزنگاری می‌کند.

۳- **دیواره‌آتش داخلی**، باید همیشه **ON** باشد، این روش محافظتی چندان سرعت اینترنت[۴۶] را کاهش نمی‌دهد اما از ورود غیرمُجاز مهاجمان به شبکه جلوگیری می‌کند.

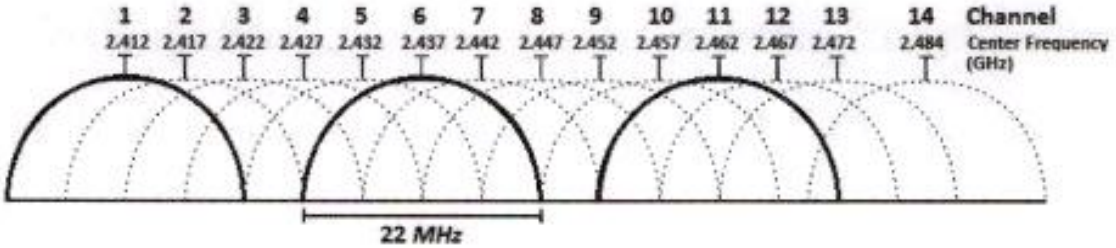
۴- **مخفی کردن SSID**[۴۷]، هر نقطه دسترسی بی‌سیم (WAP)، یک شناسه شناسایی به نام اِس‌اِس‌آی‌دی (SSID) دارد که بدون محدودیت پخش می‌شود تا به دستگاه‌های بی‌سیم امکان جستجو و شناسایی شبکه‌های بی‌سیم موجود را بدهد. دستگاه‌های بی‌سیم از این شناسه برای ایجاد اتصال توسط نقطه دسترسی به شبکه بی‌سیم استفاده می‌کنند. پنهان

[41] WEP (Wired Equivalent Privacy)
[42] WPA (Wi-Fi Protected Access)
[43] WPA Pre-Shared Key. (Temporal Key Integrity Protocol/AES)
[44] WPS (Wi-Fi Protected Setup)
[45] SAE (Simultaneous Authentication of Equals)
[46] برای اطلاع از سرعت اینترنت speedtest.net
[47] Hiding the SSID (Service Set Identifier)

کردن SSID، این نقطه دسترسی را برای هر دستگاهی نامرئی می‌کند. بدون دانستن این شناسه، کسی نمی‌تواند به شبکه متصل شود، مگر شخصی که SSID مخفی را می‌داند. با این‌حال، ابزارهای نرم‌افزاری[۴۸] می‌توانند SSIDـهای مخفی را استخراج کنند.

۵- **غربال‌کردن MAC**[۴۹]، هر کنترلر رابط شبکه (یا مبدل شبکه که در دستگاه‌ها تعبیه شده‌اند)، دارای یک شناسه سخت‌افزاری ۴۸-بیتی منحصربه‌فرد است که به مَک‌آدرس معروف می‌باشد. این مقدار را می‌توان در تنظیمات امنیتی WAPـها (مَک‌فیلترینگ) به عنوان دستگاه‌های مُجاز به دسترسی، اضافه نمود. بنابراین اتصال فقط از این دستگاه‌های مُجاز امکان‌پذیر خواهد بود. این شیوه به عنوان مکمل امنیتی عمل می‌کند و به آن نمی‌توان اتکا نمود زیرا هکرها به‌راحتی می‌توانند با کمی جمع‌آوری اطلاعات، مَک‌آدرس معتبری روی سیستم خود برای اتصال و دسترسی به شبکه تعریف کنند.

۶- **انتخاب کانال**، یکی از دلایل کاهش سرعت، فعالیت هم‌زمان شبکه‌های بی‌سیم در یک کانال مشخص است. برای مثال، در باند 2.4 GHz، یک بازه ۱۰۰ مگاهرتزی به ۱۴ کانال هر کدام با قدرت ۲۰ مگاهرتز تقسیم شده‌اند. در حالت عادی هر کانال با ۲ تا ۴ کانال دیگر همپوشانی[۵۰] دارد که این امر باعث اُفت سرعت در آن کانال‌ها می‌شود. برای داشتن یک اتصال مناسب حدالامکان از کانال‌های بدون همپوشانی ۱، ۶ و ۱۱



استفاده نمایید. به‌طور معمول WAPـها بهترین کانالی را که کمترین تداخل را داشته باشد، به‌صورت خودکار انتخاب می‌کنند. با این‌حال می‌توانید کانال‌ها را با استفاده از رابط وِب (بخش پیکربندی وای-فای[۵۱]) به صورت دستی تغییر دهید.

---

[۴۸] یا با دستور nmcli در لینوکس
[49] MAC (Media Access Control) Filtering
[50] Overlapping
[51] Wi-Fi Configuration

شبکه‌های وای-فای عمومی و رایگان، وسوسه‌انگیزند اما اگر به درستی ایمن‌سازی نشده باشند و یا کاربران بتوانند بدون احراز هویت وارد آن شوند، می‌توانند خطرناک باشند. در این نوع شبکه‌ها کاربران ناشناس (احراز هویت نشده)، ممکن است رفتارهای پرخطر مانند پخش بدافزار داشته باشند. بنابراین و در صورت امکان فقط به شبکه‌های بی‌سیمی متصل شوید که کاربران خود را قبل از اینکه مُجاز به اتصال به شبکه باشند، شناسایی می‌کنند (مانند گواهی دیجیتال برای احراز هویت). این الزامات از اتصال کاربران ناشناس و به خطر انداختن شبکه و دستگاه‌های متصل به آن، جلوگیری می‌کند.

وقتی وای-فای خود را روشن می‌کنید، فهرستی از WAP‌ـها را می‌بیند که در آن شبکه‌های بی‌سیم ناامن برچسب گذاری شده‌اند. اگر به شبکه‌ای متصل می‌شوید که ایمن نیست، توجه داشته باشید که هر شخصی با ابزارهای مناسب می‌تواند همه‌ی کارهایی که انجام می‌دهید، از جمله: بازدید از وِب‌سایت‌ها، ارسال و دریافت فایل‌ها، نام‌های کاربری و گذرواژه‌ها، و ...، را ببیند. بنابراین به پیام‌های هشداری که ممکن است دستگاه‌تان به شما بدهد، توجه ویژه‌ای داشته باشید به‌خصوص اگر نشان دهد که هویت سِرور قابل تأیید نیست. با اجتناب از چنین اتصالات ناامنی، از خودتان بیشتر محافظت می‌کنید.

نقطه دسترسی یا نقطه کانونی اتصال (هات‌اِسپات[۵۲])

در شبکه‌های بی‌سیم عمومی از AP‌ـها برای ایجاد **نقاط کانونی اتصال** جهت دسترسی به اینترنت استفاده می‌شود، که آنها را نقاط دسترسی عمومی[۵۳] یا وای-فای عمومی می‌گویند. هنگامی که در کافی‌شاپ‌ها، هتل‌ها، فروشگاه‌ها، فرودگاه‌ها، دانشگاه‌ها، کتاب‌خانه‌ها، بیمارستان‌ها یا هر مکان عمومی دیگر با لپ‌تاپ یا گوشی هوشمند خود به Wi-Fi با رمز یا بدون رمز متصل می‌شوید، در واقع در حال استفاده از یک هات‌اِسپات هستید. با اینکه به سختی می‌توان در مقابل دسترسی رایگان به اینترنت مقاومت کرد، اما نگرانی اصلی که همیشه در اتصالات وای-فای وجود دارد، **امنیت** است. در شبکه‌های Wi-Fi عمومی

[52] HotSpot
[53] Public Hotspot

انواع مختلفی از حمله‌ها در کمین کاربران هستند تا داده‌های ذخیره شده یا در حال مبادله را به سرقت ببرند. Wi-Fi-های عمومی، شبکه‌های عمومی‌اند که همه به آنها دسترسی دارند. پس باید برای هر کسی که از شبکه‌های عمومی استفاده می‌کند، حفظ اطلاعات حساس و خصوصی یک اولویت باشد. حتی اگر با رمز مستحکمی وارد شبکه شده باشید، باز هم مسائل امنیتی مهمی وجود دارند که باید به آنها توجه کنید. از جمله:

- اطلاعات شخصی خود را تنها در وِب‌سایت‌هایی وارد نمایید که به‌طور کامل رمزگذاری شده‌اند، یعنی تمام صفحات با https:// شروع شده باشند. بنابراین اگر بعد از مدتی خود را در صفحه‌ای که رمزگذاری نشده است یافتید، به سرعت از آن سایت خارج شوید.
- اگر توسط لینکی به یک سایت حتی https منتقل شدید، قبل از ادامه، آدرس اینترنتی را کپی کرده و در Notepad (یا در پرونده متنی در لینوکس و مَک) وارد نمائید و اگر محتویاتی متفاوت با آدرس مشاهده کردید، بدانید مورد فیشینگ قرار گرفته‌اید.
- مرورگرها، هنگام بازدید از وِب‌سایت‌های کلاهبرداری یا دانلود برنامه‌های مُخرب، هشدار می‌دهند. به آنها توجه کنید و مرورگر و نرم‌افزارهای امنیتی خود را به‌روز نگه دارید.
- به شبکه‌ای متصل شوید که از رمزگذاری WPA2 یا قوی‌تر از آن WPA3 استفاده می‌کند.
- هکرها با استفاده از Wi-Fi عمومی یا به وسیله‌ی کابل USB ایستگاه‌های شارژ، می‌توانند نرم‌افزارهای مُخرب وارد گوشی شما نمایند یا اطلاعات موبایل و داده‌ها را از راه سیم شارژ سرقت کنند و یا تمامی اطلاعات حساس را موقع استفاده از وای-فای عمومی شنود کنند. حتی ابزارهایی[۵۴] هستند که با آنها می‌توانند شبکه‌های Wi-Fi جعلی برپا کنند تا با ترفندهای فیشینگ شما را جذب و به سمت وِب‌سایت‌های قلابی بکشانند.

[54] e.g. wifi-pumpkin

ممکن است تمامی وِب‌سایت‌های بانکی ایمن باشند، اما در شبکه وای-فای عمومی این مکانیسم‌های امنیتی نمی‌تواند از شما در برابر حمله مرد میانی (MitM) محافظت کنند. بنابراین از هرگونه اقدامی برای خرید کالا از اینترنت یا بررسی اِیمیل باید خودداری کنید.

استفاده از نقاط اتصال همراه

با اینترنت تلفن همراه یا تبلت، می‌توانید یک نقطه دسترسی شخصی[۵۵] یا اتصال همراه[۵۶] رمزدار ایجاد کنید. این قابلیت در دستگاه‌های فوق، به شما این امکان را می‌دهند تا اینترنت آنها را با دوستان و سایر دستگاه‌ها به‌خصوص لپ‌تاپ خود به اشتراک بگذارید. این ویژگی، دستگاه را به یک WAP، شبیه به نقطه دسترسی وای-فای عمومی تبدیل می‌کند. دستگاه‌های دارای رادیو Wi-Fi می‌توانند تا زمانی که هات‌اِسپات گوشی در محدوده باشد، به آن دسترسی داشته باشند. سایر دستگاه‌ها می‌توانند از راه وای-فای، بلوتوث یا USB به هات‌اِسپات متصل شده و از آنجا به اینترنت وارد شوند[۵۷]. به همین دلیل، باید بلوتوث خود را بعد از استفاده از آن خاموش کنید، زیرا می‌تواند به عنوان یک نقطه دسترسی برای هکرها قرار بگیرد. با این‌حال، تعداد اتصالات هم‌زمان به یک وای-فای شخصی در مقایسه با وای-فای عمومی محدود است.

کارگاه آموزشی

۱- با VPN از خارج از شرکت به شبکه داخلی سازمان متصل شوید و به‌طور امن کار کنید.

۲- یکی از برنامه‌های دیواره‌آتش ص ۶۴ را انتخاب و با آن کار کنید.

۳- یک شبکه بی‌سیم راه‌اندازی کنید و تنظیمات امنیتی لازم را روی آن انجام دهید.

۴- با تلفن همراه یکی از دانشجویان، یک هات‌اِسپات راه‌اندازی و به اینترنت وصل شوید.

---

[55] Personal Hotspot (Cellular Data - iOS)
[56] Mobile Hotspot (Mobile Data - Android)
[57] Fing - Network Tools/Scanner (ابزاری برای مدیریت شبکه Wi-Fi)

فصل ۴

کنترل دسترسی

کنترل دسترسی[1] به مجموعه فنونی گفته می‌شود که مشخص می‌کنند چه کسی یا چه چیزی امکان چه کاری بر روی چه منابعی را دارد. در واقع کنترل دسترسی نوعی ایجاد محدودیت است اما برای افراد غیرمُجاز که تحت هیچ شرایطی نتوانند به منابع و اطلاعات اشخاص دیگر که متعلق به آنها نیست، دسترسی داشته باشند. برخلاف متخصصین امنیت، هکرها سعی می‌کنند با به‌کارگیری انواع بدافزارها و سؤاستفاده از آسیب‌پذیری‌های امنیتی در نرم‌افزارها به منابع و اطلاعات اشخاص دیگر دسترسی پیدا کنند.

در مباحث طراحی امنیت فیزیکی، امنیت اطلاعات و امنیت شبکه، کنترل دسترسی از موارد بنیادین برای تامین اهداف CIA و در جهت کاهش مخاطرات و ریسک‌ها است.

انواع کنترل‌ها، اقدامات و مکانیزم‌ها، و مدل‌های کنترل دسترسی را به مباحث تکمیلی و پیشرفته واگذار می‌کنیم[2]. در اینجا تنها به روش‌های جلوگیری از دسترسی غیرمُجاز به داده‌ها و آشنایی با مدیریت گذرواژها می‌پردازیم.

[1] Access Control

[2] امنیت فناوری اطلاعات - دوره پیشرفته

۱.۴ شیوه‌ها و روش‌های کنترل دسترسی

سیستم‌ها و سامانه‌ها برای شناسایی کاربران خود از یک شناسه (اسم، فامیل (یا هر دو)، نشانی اِیمیل، شماره کارمندی، و یا از شماره تلفن همراه (مرسوم در شبکه‌های اجتماعی)) به عنوان حساب کاربری[۳]، نام کاربری[۴] یا شناسه کاربری[۵] استفاده می‌کنند. این شناسه‌ها، که برای شناسایی و تعیین هویت[۶] کاربران است، یکتا می‌باشند تا بتوانند پاسخ‌گو بودن استفاده کننده را تضمین نمایند. برای تصدیق هویت و اعتبارسنجی[۷] کاربران نیز، از گذرواژه و موارد مشابه آن استفاده می‌شود. شناسایی، توأم با اعتبارسنجی را احراز هویت[۸] می‌گویند.

با اینکه اغلب کنترل دسترسی را با احراز صلاحیت[۹] یکی می‌گیرند اما ما احراز هویت و احراز صلاحیت را به عنوان دو قسمت عمده از کنترل دسترسی و زیر یک چتر در نظر می‌گیریم. در اینجا به مطالب مقدماتی احراز هویت می‌پردازیم، و بحث‌های فنی آن و همچنین احراز صلاحیت را به «دوره پیشرفته» همین مجموعه واگذار می‌کنیم[۱۰].

با این‌حال، در بسیاری از خدمات نیازی نیست که هویت کاربر مشخص شود. یعنی، در بعضی محیط‌ها ممکن است لازم باشد یا ترجیح داده شود که در گمنامی[۱۱] بمانیم!

روش‌های جلوگیری از دسترسی غیرمُجاز به داده‌ها

هکرها با به‌کارگیری انواع ابزارآلات فناوری و سؤاستفاده از شکاف‌های امنیتی در نرم‌افزارها به‌طور دائم به دنبال راه‌هایی برای سرقت اطلاعات شخصی و حمله به شبکه‌ها و سیستم‌های رایانه‌ای برای منافع مالی و شخصی هستند. در مقابل، راه‌کارهای زیادی برای اطمینان از اینکه کاربران را می‌توان در برابر انواع حملات مُخرب یا سرقت اطلاعات محافظت کرد، وجود دارد. در ادامه برخی از روش‌هایی که می‌توانید با تصدیق هویت از دسترسی غیرمُجاز به سامانه‌ها و سیستم‌های رایانه‌ای جلوگیری کنید، ذکر شده‌اند.

[3] User Account
[4] Username
[5] User ID
[6] Identification
[7] Authentication
[8] Identification & Authentication
[9] Authorization
[10] امنیت فناوری اطلاعات – دوره پیشرفته
[11] Anonymity

- **حساب‌های شبکه**[۱۲]

برای دسترسی کاربر به شبکه، به یک حساب شبکه که حقوق و مُجوزهای لازم به او اختصاص داده شده است، مورد نیاز می‌باشد. این حقوق مشخص می‌کند که کاربر مُجوز انجام چه کارهایی را در شبکه دارد. اگر حساب شبکه شما جزء گروه مدیران[۱۳] است، سطح دسترسی شما ممتاز بوده و اجازه خواهید داشت که کاربران را به رایانه، گروه و یا شبکه اضافه کنید. توصیه می‌شود زمانی که از حساب شبکه استفاده نمی‌کنید از آن خارج شوید تا بتوانید از هرگونه سؤاستفاده و آسیب تصادفی یا عمدی به داده‌ها جلوگیری کنید.

- **رمزهای عبور یا گذرواژه‌ها**

پس از شناسایی کاربر با روش نام کاربری، نوبت به اعتبارسنجی آن توسط ماشین می‌رسد تا مطمئن شود که فقط کاربران مُجاز می‌توانند به سیستم و شبکه وارد و به آنها دسترسی داشته باشند. برای جلوگیری از سرقت اطلاعات و شکسته شدن گذرواژه برای ورود به سیستم (login)، خط‌مشی‌های رمزعبور باید به شدت رعایت و اجرا شوند.

- **PIN (شماره شناسایی شخصی - پین**[۱۴]**)**

پین، نوعی رمزعبور **عددی** است که توسط کاربر برای ورود به سیستم و بیشتر در ارتباط با کارت‌های بانکی (نقدی یا خودپرداز) استفاده می‌شود. این نوع رمزعبور برای مقاصد دیگری مانند باز کردن قفل درها یا دستگاه‌های تلفن همراه و تبلت‌ها نیز به کار می‌رود.

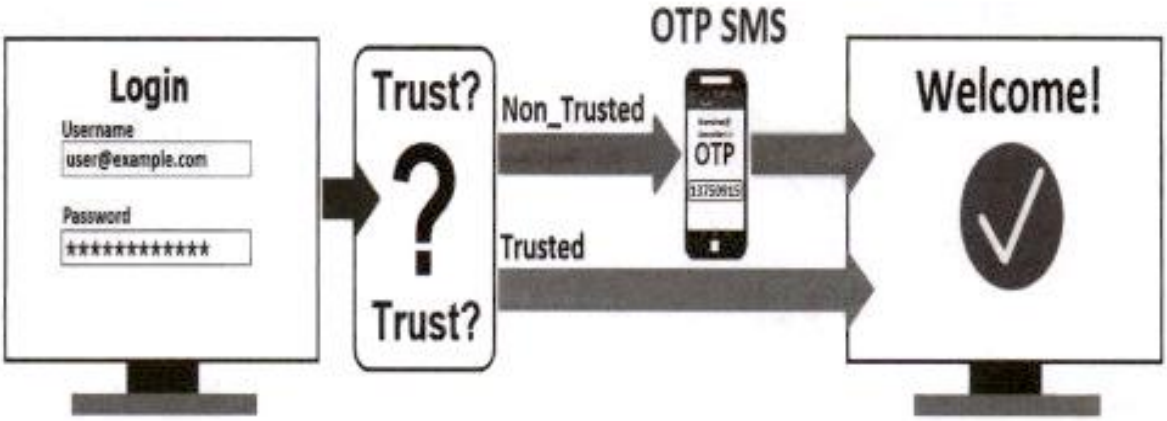
- **رمز یک‌بار مصرف** (OTP[۱۵])

با افزایش روزافزون تهدیدها (به‌دلیل آسیب‌پذیری‌ها) و حملات فیشینگ (به‌ویژه حمله مرد میانی در کلاهبرداری‌ها)، کی‌لاگرها، همچنین ترفندهای مهندسی اجتماعی در سرقت رمزهای عبور، باعث شده تا حفاظت از رمزهای ثابت در سیستم‌های بانکداری و

[12] Network Accounts
[13] Administrators
[14] PIN (Personal Identification Number)
[15] OTP (One-Time Password)

سامانه‌های حیاتی به شدت کاهش یابد. رمزهای عبور یک‌بار مصرف یا OTP لایه امنیتی اضافی همراه با احراز هویت معمول را فراهم می‌کنند.

رمز یک‌بار مصرف یا رمز پویا، نوعی رمزعبور است که اعتبار آن بر خلاف رمزهای عبور سنتی و ثابت، برای مدت زمان معینی (به‌طور معمول از ۳۰ تا ۱۰۰ ثانیه) تعریف می‌شود و تنها برای یک تراکنش یا یک‌بار ورود به سیستم (در همان مدت محدود) معتبر است. یعنی حتی اگر هکری بتواند OTP را برباید، نمی‌تواند از آن استفاده کند،



زیرا پس از ورود کاربر مُجاز به سیستم، آن رمز دیگر معتبر نخواهد بود. با این‌حال، جهت افزایش امنیت در مبادلات بانکی و خریدهای اینترنتی، علاوه بر دخالت مبلغ و شماره حساب مقصد در الگوریتم تولید OTP، می‌توان آن‌را با کُدهای پاسخ‌سریع (QR-کُدها)[۱۶] ترکیب نمود. در حال حاضر، برای بهبود امنیت در خریدهای اینترنتی و تراکنش‌های بانکی برخط، استفاده از رمزهای یک‌بار مصرف حیاتی است که با توجه به گسترش استفاده از تلفن‌های هوشمند، این‌کار به‌صورت برخط، یا با استفاده از آپ‌ها (برنامک‌های موبایلی[۱۷]) انجام می‌شود، یا از طرف بانک پیامک (SMS) می‌شود. روش دیگر تولید OTP، استفاده از توکن‌های امنیتی[۱۸] برای ایجاد پین‌های تصادفی است، که می‌توانند به عنوان سطح دوم احراز هویت عمل کنند.

[16] QR (Quick Response) code
[17] Apps (Mobile Applications)
[18] OTP Token (Security Hardware device or Software program)

- **رمزنگاری**

رمزنگاری، فنی است برای امن‌سازی اطلاعات و ارتباطات که از بهم‌ریختگی داده‌ها برای نامفهوم کردن اطلاعات استفاده می‌کند به‌طوری که برای کسی قابل فهم نباشد. این فرآیند با کمک یک عبارت به نام کلید، انجام می‌شود. کلید رمز، رشته‌ای تصادفی از نویسه‌ها (کاراکترها) است که توسط یک الگوریتم رمز به‌صورت تصادفی و منحصربه‌فرد تولید می‌شود. داده‌ها یا متن رمز شده تنها با رمزگشایی[19] توسط کلید مربوطه، قابل خواندن می‌باشند. حال، چنانچه فرد غیرمُجازی بتواند به اطلاعات یا متن رمز شده، دسترسی پیدا کند، نمی‌تواند آنها را بخواند، و فقط یک‌سری داده‌های آشغال می‌بیند.

تصدیق هویت با رمزنگاری، امضای دیجیتال[20] از نوعی رمزنگاری نامتقارن استفاده می‌کند و همان نقش امضای دستی در دنیای واقعی را ایفا می‌کند اما با امنیت بیشتر. به‌خصوص هنگامی که اسناد دیجیتال و پیام‌ها از راه یك كانال ناامن ارسال می‌شوند،

به گیرنده این اطمینان را می‌دهد که سند توسط فرد مورد نظر ارسال شده و در طول مسیر انتقال نیز دستکاری نشده است. بنابراین نه دسترسی‌های غیرمُجاز، امنیت داده را تهدید می‌کند و نه کاربر می‌تواند عملیاتی را که انجام داده است، انکار نماید.

- **تشخیص انسان از رُبات با کَپچا (CAPTCHA)**

کَپچا یک آزمایش تورینگ[21] به‌طور کامل خودکار برای کنترل دسترسی و تشخیص انسان از رایانه است، و با هدف جلوگیری از حملات نرم‌افزارهای اِسپم و رُبات‌های خودکار توسعه یافته است[22] تا کاربران حقیقی و انسانی را از آنها متمایز کند. اما رُبات‌های

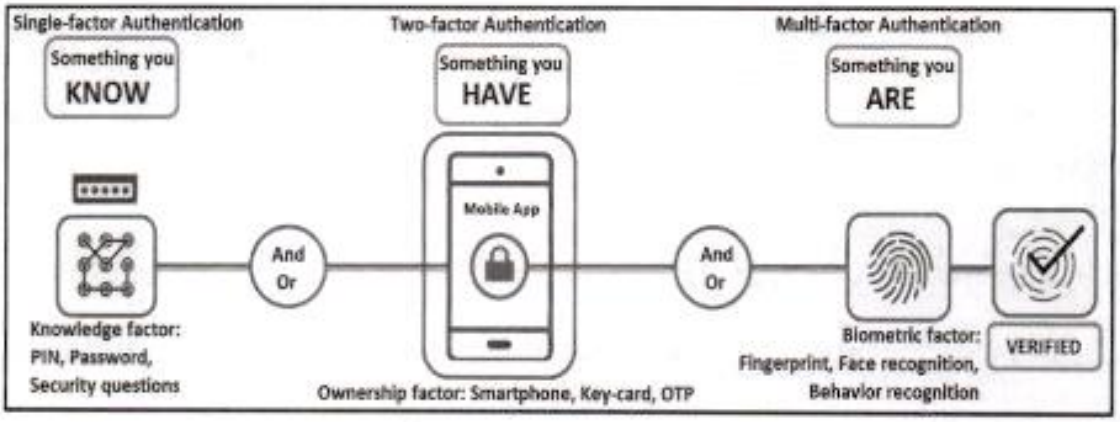
[19] Decryption
[20] Digital Signature
[21] Alen Turing (A Mathematician)
[22] توسط دانشمندان دانشگاه کارنگی ملون

پیشرفته با بهره‌گیری از قابلیت‌های یادگیری ماشین[۲۳] و هوش مصنوعی (AI[۲۴]) می‌توانند حروف و اعداد به هم ریخته را شناسایی کنند. گوگل با هدف جایگزینی کَپچای سنتی و ارتقا آن، راهکار reCAPTCHA را در سه نوع توسعه داده است:

تشخیص تصویر، کادر انتخاب[۲۵] (با I'm not a robot □)، و ارزیابی رفتار کاربر.

- **احراز هویت چند عاملی (MFA[۲۶])**

رمزعبور یا گذرواژه چیزی است که به‌طور مرتب و روزانه با آن سروکار داشته و از آن برای ایمن‌سازی رایانه‌ها، سیستم‌ها، گوشی‌های هوشمند، کارت‌ها و حساب‌های بانکی در مقابل دسترسی‌های غیرمُجاز، استفاده می‌کنید. این مکانیزم در تشخیص هویت، بیشترین کاربرد را دارد و در اصطلاح به آن تصدیق هویت تک عاملی می‌گویند. اما به عنوان ضعیف‌ترین و ناامن‌ترین عامل اعتبارسنجی در امنیت اطلاعات شناخته می‌شود. زیرا در این شیوه فقط به چیزی که **کاربر می‌داند**، اکتفا می‌شود.



برای احراز هویت کاربران مشروع، جهت دسترسی به داده‌های دارای طبقه‌بندی و برنامه‌های حیاتی، باید چیزهای دیگری نیز در نظر بگیریم تا سیستم به یک نقطه اطمینان و قابل اتکایی برسد، به‌گونه‌ایی که مطمئن شود، فردی را که در آن طرف خط و مقابل او در اینترنت نشسته همان شخصی قلمداد کند که ادعا می‌کند. پس باید علاوه بر آنچه که کاربر می‌داند، به آنچه که **دارد** یا **هست** نیز توجه کنیم.

[23] ML (Machine Learning)
[24] AI (Artificial Intelligence)
[25] CheckBox
[26] MFA (Multi-Factor Authentication)

استفاده از دو یا چند عامل اعتبارسنجی با هم را احراز هویت چندعاملی می‌نامند. با احراز هویت چند عاملی، کاربران تنها زمانی می‌توانند به یک سیستم دسترسی پیدا کنند که دو یا چند شکل از روش‌های احراز هویت را با موفقیت بگذرانند. به‌طور معمول، حداقل دو نوع از عوامل زیر مورد نیاز است:

۱. دانش، چیزی که شما می‌دانید[۲۷] (مانند گذرواژه، PIN، پاسخ سوال چالشی و ...).

۲. دارایی، آنچه که شما (همراه) دارید[۲۸] (مانند کارت عابر بانک، کارت هوشمند، OTP، تلفن هوشمند، امضاء دیجیتال، ...)، و جایی که شما هستید (مانند مکانی که از رایانه یا گوشی هوشمند استفاده می‌کنید، کشور، شهر یا آدرس IP رایانه، GPS[۲۹] و ...).

۳. ذات، چیزی که شما هستید[۳۰] (ویژگی‌های زیستی[۳۱] مانند اثر انگشت، عنبیه، چهره، هندسه دست و صورت، ...)، و رفتاری که دارید یا کاری که شما انجام می‌دهید[۳۲] (مانند سرعت تحریر رمزعبور، نحوه راه رفتن یا ریتم ضربان قلب و ...).

به عنوان مثال، کارت بانکی که شما دارید یک سیستم احراز هویت دو عاملی[۳۳] است چون برای استفاده از ATM و POS باید علاوه بر دانستن رمزعبور (عامل ۱)، کارت بانکی را نیز همراه داشته باشید (عامل ۲). استفاده از OTP در تلفن‌های هوشمند نیز نوعی احراز هویت دو عاملی مبتنی بر پیامک به حساب می‌آید.

یکی از مستحکم‌ترین شیوه‌های اعتبارسنجی، تصدیق هویت چند عاملی مبتنی بر توکن سخت‌افزاری[۳۴] است که از راه USB به رایانه وصل می‌گردد، و با افزودن یک لایه دفاعی قوی، خدمات امنیتی مورد نیاز را برای برنامه‌های کاربردی فراهم می‌نماید.

---

[27] Something (What) you know
[28] Something (What) you have
[29] GPS (Global Positioning System)
[30] Something (What) you are
[31] BioMetrics
[32] What you do
[33] 2FA (Two-Factor Authentication)
[۳۴] برای نمونه، توکن امنیتی کیا (Keya) - پیام‌پرداز

- **اعتبارسنجی با مشخصه‌های زیستی (بیومتریک)**

احراز هویت با مشخصه‌زیستی، یک روش امنیتی هوشمندانه است که برای محافظت از داده‌های فیزیکی و دیجیتالی استفاده فراوانی از آن می‌شود. ویژگی‌های فردی هر شخص نظیر اثر انگشت، الگوی عنبیه و شبکیه، گفتار، هندسه دست و صورت، و سایر جنبه‌های رفتاری و فیزیولوژیکی همگی در احراز هویت بیومتریک برای مدیریت دسترسی به سیستم رایانه‌ای یا یک محیط فیزیکی به کار می‌روند.

اعتبارسنجی بیومتریک، به‌دلیل عدم امکان به اشتراک‌گذاری مشخصه‌های زیستی فرد توسط کاربران، یکی از کارآترین و دقیق‌ترین روش‌های تشخیص هویت می‌باشد. اما مانند سایر فناوری‌ها، این روش‌ها نیز آسیب‌پذیرند و از حملات هکرها مصون نیستند، و در صورت وقوع (برای نمونه با روش‌های جعل هویت پیچیده‌ای مانند Deep fake)، در مقایسه با شیوه‌های قبلی، نتایج می‌توانند فاجعه‌آمیز و بسیار مُخرب‌تر باشند.

در این روش، هویت هر شخص بر اساس تحلیل مشخصه‌های فیزیکی فرد که به‌طور ذاتی تغییر ناپذیرند و از دقت بیشتری برخوردارند، پویش[۳۵] شده و اطلاعات حاصل از آن با داده‌های قبلی که از فرد مورد نظر ذخیره شده‌اند، مقایسه می‌شود. برای مثال، دستگاه‌های حضور و غیاب در سازمان‌ها و یا گوشی‌های هوشمند از اثر انگشت یا تشخیص چهره برای تصدیق هویت بهره می‌برند. اسکن اثر انگشت[۳۶]، تشخیص چهره[۳۷] و تشخیص صدا[۳۸] سه شیوه احراز هویت بیومتریک هستند که بیشترین کاربرد و استفاده را بین اشخاص حقیقی، شرکت‌ها و به‌خصوص تجهیزات نظامی دارند.

احراز هویت با اثر انگشت محبوب‌ترین و کم‌هزینه‌ترین روش اعتبارسنجی از این نوع است. برنامه تشخیص چهره، ویژگی‌های هندسی صورت مانند فاصله بین چشم‌ها، ارتفاع استخوان گونه‌ها و مشخصه‌های هندسی اضافی را ثبت و اندازه‌گیری می‌کند.

[35] Scan
[36] Fingerprint scan
[37] Facial Recognition
[38] Voice Recognition

تشخیص صدا، این شیوه امنیتی نیز با تطبیق الگوی صدای یک فرد با الگوی ضبط شده او کار می‌کند. تشخیص صدا با گفتار یکی نیست، زیرا گفتن کلمات، به اندازه نحوه‌ی بیان آنها اهمیت ندارند. یکی از مشکلات نرم‌افزار امنیتی تشخیص صدا این است که تغییرات صدا ناشی از حالات عاطفی، بیماری یا دلایل دیگر را در نظر نمی‌گیرد.

خطاهایی که ممکن است از اعتبارسنجی‌های بیومتریک بروز کنند، عبارتند از:

- خطای مثبت[۳۹] (یا خطای نوع اول) یعنی، عدم تایید فرد مُجاز، و
- خطای منفی[۴۰] (یا خطای نوع دوم) به معنی تایید فرد غیرمُجاز است.

وقوع خطای نوع دوم در کنترل دسترسی بسیار خطرناک است، و باید انتخاب تجهیزات و الگوریتم‌های تشخیص هویت به‌گونه‌ای باشند که به‌طور کامل از آن اجتناب شود[۴۱].

۲.۴ مدیریت رمزعبور

خط‌مشی‌های رمزعبور خوب

گذرواژه، اولین خط دفاعی شما در امنیت دیجیتال است و باید یکتا، پیچیده، طولانی و غیرقابل حدس زدن باشد، و برای جلوگیری از شکسته‌شدن رمزعبور توسط هوش مصنوعی، طول آن حداقل ۱۵ نویسه باشد. برای محافظت از سیستم‌ها در برابر دسترسی‌های غیرمُجاز، باید خط‌مشی‌ای برای ایجاد رمزعبور خوب، تدوین کرد که همه‌ی کاربران ملزم به رعایت و اجرای آن باشند. برای داشتن چنین خط‌مشی، می‌توان به دستورالعمل‌های زیر اشاره نمود:

- همیشه با ترکیب خلاقانه از (۱۰ تا ۱۵ نویسه شامل) حروف کوچک و بزرگ، اعداد و نمادهای خاص (مثل: / . , ? > < ' ; \ [] | {} + - = _ ( ) * & ^ % $ # ! @ ~)، گذرواژه‌ای قوی، که به اندازه کافی پیچیده، یکتا، ایمن و قابل حفظ باشند، بسازید. برای مثال، می‌توانید password را به‌صورت p@$$VV0rol در نظر بگیرید.

[39] False Positive-False Reject Rate
[40] False Negative-False Accept Rate
[۴۱] برای مطالعه بیشتر: www.biometrics.org

- از استفاده از کلمات موجود در فرهنگ لغت خودداری کنید.
- برنامه‌ریزی کنید گذرواژه‌ها را در فواصل زمانی منظم به‌طور مستمر تغییر دهید.
- از استفاده از رمزهای عبوری که شامل اطلاعات شخصی شما مانند نام، تاریخ تولد، نام فرزند، همسر، کُد ملی، تلفن، حیوانات خانگی، و ... می‌باشند، خودداری کنید.
- هرگز از نام‌های کاربری و گذرواژه‌های پیش فرض مشابه نمونه‌های زیر استفاده نکنید:

root, admin, 123456, 123654, qwertyuiop, password, 123123123, 123@abc, football, baseball, letmin, qwaszx, iloveyou, sunshine, moon, A123456789.

- به‌جای یادداشت‌برداری از رمزهای عبور و الصاق یا چسپاندن آنها زیر مانیتور یا روی میزکار، از نرم‌افزارهای مدیریت رمز[۴۲] استفاده کنید.
- از رمزعبور یکسان برای خدمات یا سیستم‌های مختلف استفاده نکنید.
- هرگز رمزعبور خود را به کسی ندهید، فاش نکنید یا به اشتراک نگذارید.

نرم‌افزار مدیریت رمز

برنامه‌های مدیریت رمز[۴۳]، به شما کمک می‌کنند گذرواژه‌های پیچیده و امن تولید و آنها را به همراه سایر اطلاعات مورد نیاز برای ورود به سایت‌های مختلف، در یک محیط امن و غیرقابل نفوذ ذخیره و مدیریت نمایید. حتی به شما کمک می‌کنند تا در صورت لزوم به‌طور خودکار به آن سایت‌ها وارد شوید. به‌خاطر حساسیت ویژه این نوع برنامه‌ها، رمزعبور خود آنها حداقل به‌صورت دوعاملی طراحی شود، اما آگاه باشید که آنها هم خطاناپذیر نیستند.

کارگاه آموزشی

۱- با حساب کاربری، وارد شبکه شوید و ببینید چه منابعی به اشتراک گذاشته شده‌اند.

۲- یکی از برنامه‌های مدیریت رمز در ص ۸۰ را انتخاب و با آن کار کنید.

[42] Password Management Softwares

[43] KeePassXC, Bitwarden, Dashlane, LastPass, ...

فصل ۵

استفاده امن از وِب

۱.۵ مرورگرهای وِب

شبکه جهانی وِب (WWW) یا به اختصار **وِب**، یک سیستم اطلاعاتی است که امکان دسترسی به اسناد و سایر منابع وِب را از راه اینترنت فراهم می‌کند. معماری وِب به صورت Client-Server طراحی شده است. اطلاعات در سمت سرویس‌دهنده در وِب‌سِرورها[1] ذخیره می‌شوند، وِب‌سایت‌هایی[2] که نقش خبرگزاری، دفتر کار، بانک یا بیمه را ایفاد می‌کنند و گاهی پایگاهی برای پخش خدمات ویدئویی می‌شوند و در سوی دیگر، مشتریانی قرار دارند

که بی‌صبرانه مشتاق دریافت این اطلاعات و خدمات هستند.

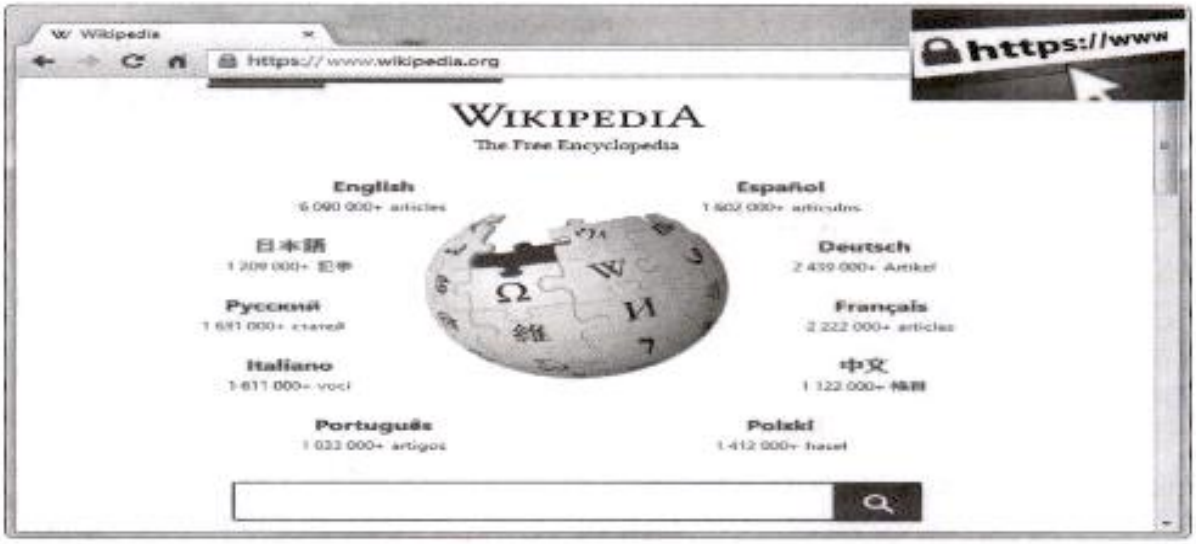
برای دسترسی به اطلاعات وِب‌سایت‌ها، از برنامه‌ایی به نام مرورگر وِب[3] استفاده می‌شود. مرورگر یا کاوشگر[4] یک برنامه نرم‌افزاری است که با استفاده از آن می‌توان اسناد و صفحات

---

[1] Web Servers
[2] Web Sites
[3] Web Browser
[4] Explorer

وِب (شامل متن، تصویر، صوت، ویدئو و سایر محتویات چندرسانه‌ای) را مشاهده و به کمک ابَرپیوندها[5] در میان آنها حرکت کرد. مرور وِب را گشت‌وگذار یا وِب‌گردی می‌نامند. وِب یکی از کاربردهای اصلی اینترنت می‌باشد و نمی‌توان این دو را با هم یکسان گرفت. اکثر مرورگرها در رایانه‌های رومیزی[6] و بیشتر دستگاه‌های همراه[7] به خوبی کار می‌کنند. اما برخی از دستگاه‌ها مانند کنسول‌های بازی[8] مرورگرهای خاص خود را دارند.

نوار آدرس[9] در بالای صفحه مرورگر، جایی که نشانی وِب[10] را در آن وارد می‌کنید، و نوار وضعیت[11] در پایین صفحه مرورگرها، اهمیت ویژه‌ای دارند. نوار آدرس، نشانی اصلی



صفحه‌ی در حال نمایش و وضعیت امنیتی و رمزگذاری صفحات وِب (علامت قفل و https://) را نشان می‌دهد و نوار وضعیت هم به شما می‌گوید، وقتی نشانگر روی یک پیوند (لینک) قرار بگیرد آن ارتباط به چه آدرس واقعی اشاره می‌کند. این نوار در شناسایی لینک‌ها و صفحات مشکوک اهمیت بسیار زیادی دارد و قبل از کِلیک بر روی پیوندها، درنگ کرده و با دقت بیشتری به محتوای نمایش داده شده توجه کنید، تا فریب نخورید.

خدماتی نظیر دولت الکترونیکی، آموزش مَجازی، بازاریابی و تجارت الکترونیک در کنار بانکداری دیجیتال، شبکه‌های اجتماعی، سرگرمی و بازی تنها گوشه‌هایی از اهمیت این

[5] HyperLinks
[6] Linux, Windows, MacOs, ...
[7] Android/iPhone/iPad, ...
[8] PlayStation, XBox, Nintendo Switch
[9] Address Bar
[10] URL (Uniform Resource Locator)
[11] Status Bar

فناوری را نشان می‌دهد. در واقع، نرم‌افزار وِب را می‌توان رابط کاربری برای استفاده از اینترنت دانست که باعث شده میلیاردها کاربر و دستگاه بتوانند به‌راحتی به زیرساخت‌های شبکه اینترنت متصل شوند و به منابع عظیم اطلاعاتی ذخیره شده دسترسی یابند و به‌طور قطع بدون آن، این حجم استفاده از اینترنت ممکن نبود.

۲.۵ تنظیمات مرورگر

مرورگرها برای افزایش قابلیت‌های خود، از فناوری‌هایی استفاده می‌کنند که بالقوه آنها را در معرض دسترسی‌های غیرمُجاز یا اجرای کُدها و برنامه‌های مُخرب قرار می‌دهند. در واقع، بیش از ۸۰ درصد از سیستم‌ها از راه وِب به بدافزار آلوده می‌شوند. به‌طور کلی، مرورگرها با تنظیمات و پیکربندی پیش‌فرض به خوبی کار می‌کنند اما برخی از تنظیمات و ترفندها وجود دارند که امکان وِب‌گردی راحت‌تر و ایمن‌تری را فراهم می‌کنند. این تنظیمات شامل تنظیمات کلی، تنظیمات شخصی و تنظیمات امنیتی و حفظ حریم‌خصوصی می‌باشند.

برای کاهش مشکلات امنیتی و حفظ حریم‌خصوصی باید متناسب با شغل و حرفه خود تنظیمات مناسب را انتخاب یا پیکربندی کنید. محل این تنظیمات یا حتی اصطلاحات به کار رفته از یک مرورگر به مرورگر دیگر یا حتی از یک نسخه به نسخه دیگر (رایانه و گوشی)، ممکن است فرق کند. برای اطلاعات بیشتر به راهنمای آن توزیع مراجعه کنید. اما مرسوم‌ترین و مهمترین این تنظیمات عبارتند از:

- فعال یا غیرفعال کردن جاوا اسکریپت و کوکی‌ها (Enable Javascript / Cookies)،
- مسدود کردن یا اجازه اجرای پنجره‌های بازشونده (Settings: (Block) Pop-ups)،
- فعال یا غیرفعال کردن تکمیل خودکار فیلدها[۱۲]، به‌ویژه برای نام‌کاربری و رمزعبور،
- پاک کردن اطلاعات خصوصی از مرورگر (Clear Browser Cache / History)،

[12] Autofill

- فعال یا غیرفعال کردن موقعیت جغرافیایی، میکروفن و دوربین (وِب‌کَم[۱۳])،
- تنظیم صفحه خانگی[۱۴] به عنوان اولین صفحه‌ای که با اجرای مرورگر باز می‌شود.

جاوا اسکریپت

یک زبان برنامه‌نویسی مهم و کاربردی است و با قابلیت‌های فوق‌العاده‌ای که دارد می‌تواند صفحات وِب را پویاتر و جذاب‌تر کند. می‌تواند برخی از قسمت‌های صفحه را بدون بارگذاری کامل آن، به‌روز کند. یا زمانی که اطلاعات ورود به سیستم را ناقص وارد می‌کنید، به شما پیغام می‌دهد «نام کاربری یا رمزعبور را وارد نکرده‌اید.». همچنین به‌روز رسانی لحظه‌ای خبرخوان‌ها با جاوا اسکریپت است. اما امنیت پایینی دارند و به‌راحتی می‌توانند مورد سؤاستفاده مهاجمین قرار بگیرند. بسیاری از وِب‌سایت‌ها بدون جاوا اسکریپت به درستی (یا اصلاً) کار نمی‌کنند. بنابراین در فعال یا غیرفعال کردن آن احتیاط کنید.

کوکی‌ها (کلوچه‌های اطلاعات)

کوکی یک فایل متنی است که مرورگر هنگام مشاهده وِب‌سایت، وضعیت جلسه و برخی اطلاعات دیگر را به درخواست آن سایت بر روی رایانه (موبایل یا تبلت) شما ذخیره می‌کند. تا بتواند کاربران خود را شناسایی کرده و به سوابق و سایر علاقه‌مندی‌های او پی ببرد.

مسدود کردن پنجره‌های بازشونده

ابزارهای تبلیغاتی پنجره‌های pop-up، که با اطلاع، انتخاب و کنترل کاربر فعالیت می‌کنند، فریبنده نبوده و نباید به عنوان ابزار جاسوسی در نظر گرفته شوند. با این‌حال، تبلیغات پنجره‌های بازشونده گاهی اوقات آزاردهنده می‌شوند و در برخی موارد کارآیی سیستم را به شدت کاهش می‌دهند. همچنین اطلاعاتی که برخی از آنها جمع‌آوری می‌کنند ممکن است محدوده حریم خصوصی افرادی که آگاهی کافی از مفاد موافقت‌نامه را ندارند نقض کنند، در چنین شرایطی توصیه می‌شود که آنها مسدود شوند.

[13] Webcam(-era)
[14] Home page

تنظیم گزینه‌های تکمیل خودکار فیلدها

مرورگرها دارای ویژگی تکمیل خودکار در فیلدهای متنی هستند که به شما امکان می‌دهد نام‌های کاربری، گذرواژه‌ها و سایر اطلاعات را ذخیره کنید و سپس می‌توانید، از این ویژگی برای پُرکردن خودکار فرم‌های برخط استفاده کنید. برای مثال، هنگام ورود به وِب‌سایت‌های پُرکاربرد، نام کاربری و رمزعبور شما به‌طور خودکار موقع بارگیری صفحه وِب برای شما پُر می‌شود. این ویژگی صرفه‌جویی در زمان، هنگام استفاده در رایانه‌های شخصی مفید است. اما در رایانه‌های مشترک یا عمومی، ممکن است این قابلیت، حریم‌خصوصی شما را نقض کند و نخواهید که این اطلاعات برای استفاده کسی ذخیره شود. در چنین شرایطی، می‌توانید برخی از ویژگی‌های تکمیل خودکار را برای پیشگری از افشای اطلاعات، غیرفعال کنید.

پاک کردن اطلاعات خصوصی از حافظه نهان و تاریخچه مرورگر

مرورگرها، اطلاعات مربوط به وِب‌سایت‌هایی که بازدید می‌کنید و همچنین اطلاعاتی را که اغلب از شما درخواست می‌کنند (مانند نام، آدرس و ...) در دیسک‌سخت رایانه تحت عنوان حافظه نهان ذخیره می‌کنند. مرورگرها از این ترفند برای بارگذاری سریع‌تر صفحاتی که تغییر نکرده‌اند، استفاده می‌کنند و با توجه به اندازه حجم حافظه نهان، این اطلاعات می‌توانند تا مدت‌ها روی رایانه باقی بمانند. اگر از رایانه‌های عمومی در مکان‌هایی مانند کتاب‌خانه‌ها، کافی‌نت‌ها و ...، استفاده می‌کنید و نمی‌خواهید هیچ‌یک از جزئیات شخصی شما باقی بماند، باید آنها را به‌طور اصولی حذف کنید. برخی از این اطلاعات عبارتند از:

- فایل‌های موقت اینترنتی، - کوکی‌ها، - تاریخچه وِب‌سایت‌هایی که بازدید کرده‌اید،
- اطلاعاتی که در وِب‌سایت‌ها یا نوار آدرس وارد کرده‌اید، و
- رمزهای عبور ذخیره شده در وِب.

بنابراین اگر برای تراکنش‌های مالی و بانکی از وِب استفاده می‌کنید، اطلاعات محرمانه شخصی شما (یعنی اطلاعات خرید، کارت‌های اعتباری، حساب‌های بانکی، اِیمیل و ...)

در آن رایانه (تبلت یا موبایل) به‌طور کامل قابل خواندن و بازیابی خواهند بود، و پس از پایان کار باید حافظه نهان و تاریخچه مرورگر را پاک نمایید، تا مورد سؤاستفاده قرار نگیرید.

Chrome => Settings> Privacy and Security> Site settings>
JavaScript / Cookies and site data / Pop-ups (Block/Allow)

Safari => Preferences> Security> ☐ Enable JavaScript/ ☐ Block pop-up
Preferences> Privacy> Block cookies

Firefox => URL:"about:config">Type "javascript">"javascript.enabled"
URL:"about:preferences">Privacy & Security>Cookies/pop-up ...

Edge => Settings> Site permissions> JavaScript/Cookies and site data

برای آگاهی از وضعیت تنظیمات امنیتی مرورگر، می‌توانید از سایت زیر کمک بگیرید:

https://www.whatismybrowser.com/ .

اگر کنترلی روی کوکی‌ها یا حافظه نهان مرورگر ندارید (مانند رایانه‌های اماکن عمومی، کتاب‌خانه‌ها، مدارس، و ...) هرگز اطلاعات خصوصی، مالی و بانکی خود را وارد نکنید.

تنظیم صفحه خانگی

بعضی از بدافزارها به‌خصوص آنهایی که برای اهداف تبلیغاتی طراحی می‌شوند بدون اجازه کاربر، صفحه خانگی مرورگر را تغییر می‌دهند، یا مرورگر را مجبور می‌کنند صفحاتی را نمایش بدهد که عمدتاً با هدف کسب درآمد از وِب‌گردی شما برنامه‌ریزی شده‌اند. با اینکه ممکن است این صفحات بی‌ضرر به نظر برسند اما در هر صورت، بیانگر عفونی بودن سیستم شما است و این امر به‌ویژه هنگام ورود به سایت‌های بانکی برای انجام امور بانکی و مالی، یا فروشگاه‌های اینترنتی برای خرید برخط (آنلاین)، بسیار خطرناک خواهد بود.

۳.۵ گشت و گذار امن در فضای وِب

وقتی وارد عمارت شیشه‌ایی فضای مَجازی می‌شوید، باید دو نکته مهم را همواره به‌خاطر بسپارید: ۱- وارد شبکه‌ی ناامن و غیرقابل اعتمادی به نام اینترنت شده‌اید.

۲- هوشیار باشید قبل از کِلیک بر روی هر پیوندی، چند لحظه مکث کنید و نوار وضعیت را ببینید. آیا این نشانی، همان مقصد مورد ادعا است؟

پس وقتی که یک صفحه وِب از شما اطلاعات حساسی را درخواست می‌کند، باید بتوانید تشخیص دهید که آیا آن صفحه امن است یا خیر؟[۱۵] توانایی تشخیص یک اتصال وِب ایمن بسیار مهم است زیرا فعالیت‌های برخط تجاری مانند خرید اینترنتی یا تراکنش‌های مالی و بانکی فقط باید در صفحات وِب امن انجام شود، در غیر این صورت به‌راحتی مورد سؤاستفاده و کلاهبرداری قرار می‌گیرید. مشکلاتی که ممکن است وِب‌سایت (یا تارگاه) ناامن برای شما پیش بیاورد، عبارتند از:

- آلوده نمودن سیستم به بدافزارها، ویروس‌ها، باج‌افزارها، ...، و زامبی کردن شما،
- نقض حریم خصوصی و افشای اطلاعات محرمانه شخصی (شنود و حملات MitM)،
- امکان ارسال هرزنامه یا اِسپم به شما و مخاطبان شما.

برای بررسی ایمنی وِب‌سایت و محافظت از خود، می‌توانید از اقدامات زیر استفاده کنید:

- **اطمینان از امنیت ارتباطی سایت**

در طول نشست و در نوار آدرس تمام صفحات باید https:// و علامت قفل بسته باشد.

- **نشانی وِب یا URL معتبر**

اگر می‌خواهید اینترنتی خرید کنید و شرکتی، کالاها را از راه میزبانی وِب‌سایت‌های معتبر (مانند eBay، آمازون یا ...) می‌فروشد، حتماً URL آن سایت‌ها را بررسی کنید (نوار وضعیت را ببینید) که آیا به وِب‌سایت واقعی اشاره می‌کند یا خیر؟

---

[۱۵] باید عبارت https:// در ابتدای نشانی باشد

- **کیفیت و شهرت محتوا**

اگر وِب‌سایتی (و محتوای آن) در مدت زمان قابل توجهی به‌روز نشده باشد، احتیاط کنید ممکن است استفاده از خدمات آن به‌خصوص اگر اطلاعات حساسی بخواهد، ایمن نباشد. کیفیت محتوا، شهرت و ادبیات به کار رفته، اغلب شاخص خوبی برای مشروع بودن یا نبودن یک وِب‌سایت به حساب می‌آید.

- **بررسی گواهی امنیتی و تأیید اعتبار مالک دامنه**

در نوار آدرس مرورگر، برای مثال در کروم (Chrome) با کِلیک بر روی نماد قفل و سپس انتخاب Certificates، می‌توانید گواهی امنیتی وِب‌سایت و اعتبارنامه مالک دامنه را بررسی کنید. همچنین می‌توان با استفاده از وِب‌سایت‌هایی مانند www.mywot.com، میزان قابل اعتماد بودن دامنه وِب‌سایت و تأییدیه مالک آن‌را مشاهده کنید.

فارمینگ[۱۶]

فارمینگ مانند فیشینگ، تهدیدی است که کاربران را فریب می‌دهد تا اطلاعات شخصی خود را فاش کنند. اما بر خلاف آن، به‌جای اتکا به اِیمیل به عنوان بُردار حمله برای گول زدن یک کاربر، از روش زیرکانه‌تری استفاده می‌کند. مهاجمان در این شیوه، سعی می‌کنند آدرس IP شبکه یا سِرورهای DNS[۱۷] را برای متوقف کردن تمامی کارکرد آن مورد حمله قرار دهند، تا بتوانند به‌صورت مستمر و مخفیانه تعداد زیادی از قربانیان را به سمت وِب‌سایت‌های جعلی خود هدایت کنند، حتی اگر قربانی، آدرس وِب‌سایت مقصدش را درست وارد کند!

فایل میزبان[۱۸]، وظیفه ترجمه نام دامنه (اسامی کاربرپسند گره‌ها مثل www.host.com) را به آدرس‌های پروتکلی عددی (مانند IP: x.x.x.x) دارد. هنگامی که آدرس سایتی را در مرورگر وارد می‌کنید، رایانه (یا سیستم عامل) ابتدا به فایل میزبان محلی خود مراجعه می‌کند و آدرس IP نگاشت شده به آن URL را استخراج، و آن‌را به مرورگر تحویل می‌دهد.

[16] Pharming (Phishing-Farming)
[17] DNS (Domain Name System) Server
[18] Hosts file

مرورگر از این شماره IP برای برقراری اتصال به سایت مورد نظر استفاده می‌کند. اما اگر IP و سایت مربوطه، در این پرونده نباشند، آنگاه رایانه برای ایجاد ارتباط به سراغ سِرورهای DNS (سیستم نام دامنه) سازمان یا اینترنت می‌رود و آی‌پی را در آنها جستجو می‌کند.

Linux: $ sudo cat /etc/hosts
MacOS: $ sudo nano /private/etc/hosts
Windows: C:\type C:\Windows\System32\drivers\etc\hosts

```
# 127.0.0.1          localhost (is called the loopback address and refer to itself)
# ::1                ip6-localhost ip6-loopback (IPv6, ::1 i.e 0:0:0:0:0:0:0:1)
# 0.0.0.0 -or- 127.0.0.1 google.com  i.e  #ThisWillTrytoBlock google.com
# 255.255.255.255    broadcasthost
127.0.0.1            localhost
::1                  ip6-localhost
142.250.186.68       www.yourdomain.com  yourdomain.com
```

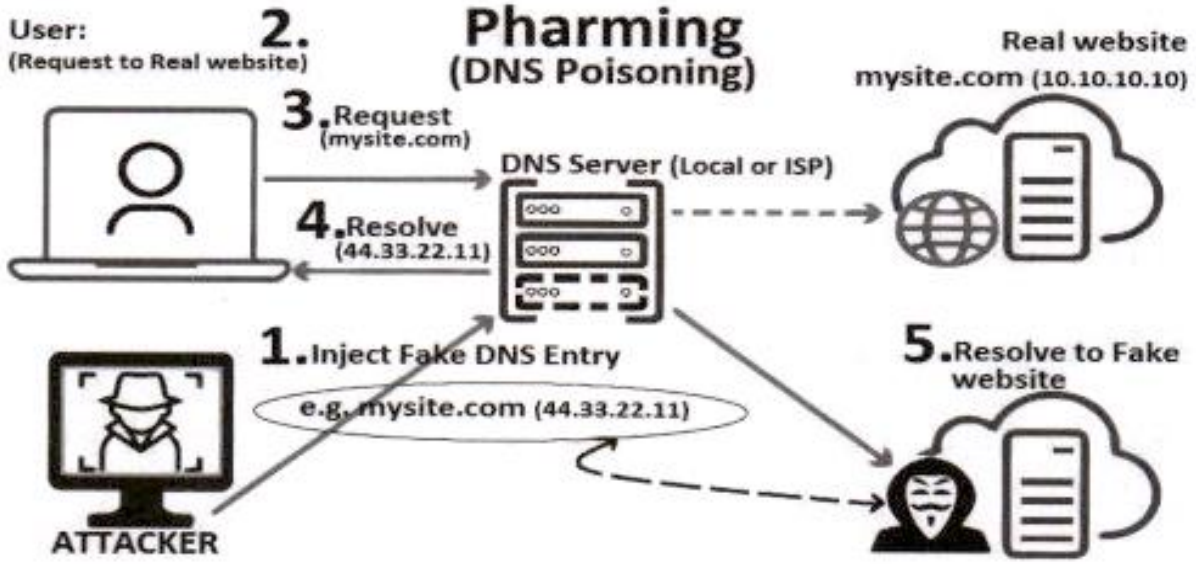
نقش DNS مشابه فایل hosts (تبدیل نام و نشانی URL به عدد منحصربه‌فرد IP) است، منتها با قابلیت‌های بیشتری و در سطح گسترده‌تری از شبکه‌ها و اینترنت عمل می‌کند. حمله فارمینگ به دو صورت انجام می‌شود:

- **اول، دستکاری فایل-میزبان در رایانه قربانی**
  در این حمله‌ها، نفوذگران از بدافزارهای تروجان، برای نصب برنامه‌های کلیدخوان و هدایت‌کننده استفاده می‌کنند و یا کُدی به‌صورت اِیمیل برای قربانی ارسال می‌شود که حاوی فایل‌های میزبان محلی با محتویات مُخرب و تحریف شده می‌باشد تا با جایگزینی او با فایل اصلی، قربانی را به وِب‌سایت‌های جعلی مورد نظر مهاجم بکشاند.
- **دوم، بهره‌برداری از آسیب‌پذیری سِرورهای DNS**
  این روش به حمله مسموم کردن یا گمراه‌سازی DNS[19] معروف می‌باشد. در این روش هدف اصلی مهاجم از حمله[20] به سِرورهای DNS آن است که با مسموم کردن اطلاعات[21]، بتواند یک IP مُخرب از نشانی وِب‌سایت مورد نظرش را به‌جای IP معتبر تزریق کند. در این شیوه از فارمینگ، نیازی به تغییر فایل‌های میزبان در رایانه‌های شخصی نیست،

[19] DNS (Cache) Poisoning/Spoofing
[20] e.g. with DNS Changer Virus
[21] یعنی، با دستکاری و تغییر داده‌ها (آلوده کردن)

در عوض، مشکل در قسمت DNS-سِرور اتفاق میفتد. جایی که میلیون‌ها کاربر اینترنت درخواست یک سری URL دارند و در این بزنگاه است که مهاجمان می‌توانند به تعداد زیادی از کاربران حمله کنند. زیرا جدول سیستم نام دامنه در سِرور به‌گونه‌ای تغییر یافته که کاربران حتی با وارد کردن URL معتبر، خودکار به سایت‌های متقلب هدایت می‌شوند.

نمودار زیر، چگونگی یک حمله فارمینگ معمولی را نشان می‌دهد.



۱. مهاجم، DNS سرویسی را که برای مثال توسط ISP میزبانی می‌شود، هدف قرار می‌دهد. هکر IP-آدرس (10.10.10.10) وِب‌سایت mysite.com، را به IP-آدرس (44.33.22.11)، وِب سِروری که نسخه جعلی همان وِب‌سایت (mysite.com) است، تغییر می‌دهد.

۲. کاربر می‌خواهد به وِب‌سایت (mysite.com) برود و آن‌را در نوار آدرس تحریر می‌کند.

۳. رایانه کاربر از سِرور DNS، IP-آدرس وِب‌سایت (mysite.com) را سؤال می‌کند.

۴. از آنجایی که سِرور DNS از قبل توسط مهاجم **مسموم** شده است، او IP-آدرس وِب‌سایت جعلی (44.33.22.11) را به عنوان آدرس سایت اصلی، به رایانه کاربر برمی‌گرداند.

۵. رایانه کاربر، پاسخ تقلبی (IP: 44.33.22.11) را دریافت و آن‌را به عنوان IP-آدرس صحیح وِب‌سایت mysite.com تفسیر می‌کند. حال، کاربر فریب خورده و به‌جای وِب‌سایت اصلی، به وِب‌سایت جعلی که تحت کنترل مهاجم است، کشانده می‌شود.

دقت کنید در این گرداب حتی اگر کاربر آدرس URL سایت اصلی را صحیح وارد کند یا روی لینک‌های معتبر کِلیک کند، باز هم قربانی شده! و به سایت‌های جعلی و کلاهبرداری هدایت می‌شود، آن هم بدون هیچ علائم یا نشانه‌ای که بتواند اختلاف سایت اصلی را از تقلبی تشخیص دهد. با این‌حال، برخی از نرم‌افزارهای ضدجاسوسی می‌توانند انحراف ایجاد شده در کُدهای فایل-میزبان را تصحیح کنند. اما اگر کاربر عادت‌های جستجوی خود در اینترنت را عوض نکند، یا ملاحظات و سیاست‌های ایمنی کار با رایانه‌ها را رعایت نکند، از نام‌ها و رمزهای عبور پیش‌فرض استفاده کند و یا فایروال را خوب و امن پیکربندی نکند، این حمله‌ها تکرار می‌شوند. البته حملات DNS Poisoning نیازمند دانش زیادی بوده و به سادگی قابل انجام نیست. به هر حال DNS-سِرورهایی که از لایه‌های امنیتی مناسبی برخوردار نبوده و آسیب‌پذیر باشند، مستعد انجام چنین حمله‌ای خواهند بود.

فیشینگ هموگراف[۲۲]، روی پیوندی که به وسیله‌ی اِیمیل برای شما ارسال شده است کِلیک می‌کنید و وارد وِب‌سایت https://wikipedia.org می‌شوید. مرورگر با نمایش علامت قفل سبزرنگ، امن بودن این ارتباط را تائید می‌کند و شما با اطمینان و اعتماد بیشتری به مرحله بعد می‌روید. اما در اینجا حروف «e» و «a» با خط سیریلیک[۲۳] روسی «e» و «a» جابه‌جا شده‌اند، و شما با آدرس (URL) جعلی و با استفاده از یونیکُد[۲۴] دچار حمله فیشینگ شده‌اید. اکثر مرورگرها، برای نمایش نویسه‌های یونیکُد، به‌طور پیش‌فرض از کُدگذاری کوتاه‌شده[۲۵] استفاده می‌کنند، و به‌جای نویسه‌های واقعی، نتیجه کُدگذاری شده

[22] Homograph phishing
[23] Cyrillic script
[24] Unicode
[25] Punycode Encoding

را در نوار آدرس نمایش می‌دهند.**توجه کنید:** گواهی‌نامه امنیتی فقط وجود یک ارتباط امن با سایت مورد نظر را تائید می‌کند، اما در رابطه با اینکه آیا وارد سایت مُجاز شده‌اید یا نه، چیزی به شما نمی‌گوید! همچنین وِب‌سایت‌های قانونی هیچ‌وقت در صفحات خود لینک سایت خود را درج نمی‌کنند. روش‌هایی که برای پیش‌گیری از فارمینگ مؤثرند، عبارتند از:

۱- یکی از مهمترین و مؤثرترین روش‌ها، بررسی گواهی‌نامه امنیتی وِب‌سایت است،
۲- نشانی (و یا شماره IP) وِب‌سایت را در نوارآدرس به‌صورت دستی وارد کنید،
۳- نشانگر را روی لینک برده و با دقت به محتوای آن در نوار وضعیت توجه کنید،
۴- از یک Link Scanner برای بررسی پیوند استفاده کنید. اینها وِب‌سایت‌هایی هستند که با استفاده از نرم‌افزارهای ضدویروس مبتنی بر اَبر، بی‌خطر بودن بازدید از یک لینک را برای وجود محتوای مُخرب بررسی می‌کنند.

مدیریت محتوا

نرم‌افزار کنترل محتوا[۲۶] که به سانسورافزار[۲۷] یا فیلترینگ اینترنت[۲۸] نیز شناخته می‌شود، برنامه‌ایی است که برای محدود کردن یا کنترل محتوایی که کاربر هنگام مرور وِب، مُجاز است به آن دسترسی داشته باشد، طراحی و بهینه شده است. یعنی، تنظیم‌کننده مقررات با این برنامه‌ها، تصمیم می‌گیرد که چه سایت‌ها یا محتواهایی در دسترس باشند یا مسدود شوند. چنین محدودیت‌هایی را می‌توان در سطوح مختلفی از مخاطبان اِعمال کرد:

دولت برای کل کشور، به وسیله‌ی فراهم‌کننده خدمات اینترنت (ISP) برای مشتریانش، سازمان برای کارکنان خود، مدرسه برای دانش‌آموزانش، برای فرزندان توسط والدین[۲۹]، یا توسط خود کاربر برای رایانه شخصی خودش. هنگامی که کنترل محتوا بدون رضایت کاربر تحمیل شود، آن‌را سانسور اینترنتی می‌نامند. در مقابل، فناوری‌هایی که امکان شکستن این محدودیت را فراهم می‌آورند، به آنها فیلترشکن می‌گویند[۳۰].

[26] Content-control software
[27] Censorware
[28] Internet Filtering
[29] Parental Control
[۳۰] مانند VPN‌ـها

انواع فیلترینگ

براساس خط‌مشی‌های کنترلی، فیلترینگ را به روش‌های مختلفی می‌توان پیاده‌سازی کرد، اما هیچ راه حلی، پوشش کاملی را فراهم نمی‌کند.

- **فیلترهای سمت مشتری**[۳۱]

این نوع فیلتر به عنوان نرم‌افزار، روی هر رایانه‌ای نصب می‌شود و توسط هر فردی که دارای امتیازات دسترسی سطح مدیر[۳۲] در سیستم است قابل مدیریت و شخصی‌سازی می‌باشد. این برنامه‌ها اغلب توسط والدین برای نظارت و کنترل دسترسی کودکان به محتوای نامناسب در اینترنت استفاده می‌شوند.

- **فیلترهای مبتنی بر مرورگر**[۳۳]

این روش، سبک‌ترین راه حل برای فیلتر محتوا است و توسط افزونه‌ها و یا پلاگین‌هایی انجام می‌شود که می‌توانند به مرورگر اضافه شوند.

- **فیلتر محتوا در سطح ISP**[۳۴]

برخی از فراهم‌کنندگان خدمات اینترنتی (ISP) به‌صورت انتخابی یا اجباری فقط به بخشی از محتوای وِب دسترسی دارند، یا ترافیک وِب را براساس قوانین تعیین شده از سوی دولت یا سازمان متولی تنظیم مقررات، محدود می‌کنند. هنگامی که ISP فیلترینگ محتوا را پیاده‌سازی می‌کند، این محدودیت بر روی تمام مشترکان او تاثیر می‌گذارد.

- **فیلترهای موتور جستجو**[۳۵]

بسیاری از موتورهای جستجو به کاربران این امکان را می‌دهند که فیلتر ایمنی را روشن کنند تا لینک‌های نامناسب را از تمام نتایج جستجو پاک کند. اگر کاربری URL واقعی وِب‌سایتی را بداند، می‌تواند (با تحریر آن در نوار آدرس) بدون استفاده از موتور جستجو به آن محتوا دسترسی پیدا کند. استفاده از موتورهای جستجوی ایمن ویژه کودکان[۳۶]، به

[31] Client-side filters
[32] Administrator-level privileges
[33] Browser-based filters
[34] ISP-level content filter
[35] Search-engine filters
[36] Kiddle, KidRex, kidzSearch, Boolify, Dib Dab Doo, FactMonster, WackySafe, ...