جزوه امنیت سایبری

راهکارها و تهدیدات

تهدیدات سایبری و راهکارهای دفاعی

تهیه کننده:

دکتر محمدرضا دهقانی محمودآبادی

مهر ۱۳۹۹


بسم الله الرحمن الرحیم

چکیده

ناکامی در عرصه تهدیدهای سخت و هزینه بر بودن آن، موجب تغییر راهبرد دشمنان نظام اسلامی شد. استفاده از ظرفیت‌های موجود در فضای سایبری به عنوان راهبرد تقابل با ج.ا. ایران، در کانون توجه استکبار جهانی قرار دارد. هدف شناسایی و ارزیابی تهدیدهای سایبری در دو حوزه نرم و سخت، آسیب‌های موجود، فرصت‌های مقابله و ارائه راهکار است. به این منظور، مؤلفه‌های اساسی در حوزه تهدیدها، آسیب‌ها و فرصت‌ها مورد ارزیابی قرار گرفت. تحقیقات نشان داد ابعاد اقتصادی، امنیتی و نظامی بیشترین اثرپذیری را در برابر تهدیدهای سایبری دارند و مهم‌ترین آسیب پذیری ها، استفاده از تجهیزات غیربومی و عدم رعایت پدافند غیرعامل است. همچنین با توجه به نظر خبرگان، در حوزه فناوری، رعایت امنیت فضای تبادل اطلاعات، توسعه مراکز عملیات امنیت شبکه و انتقال مراکز نگهداری داده به داخل کشور پیشنهاد و در حوزه نیروی انسانی، الگویی برای شناسایی، توانمندسازی و شبکه سازی فعالان عرصه فضای سایبری ارائه گردید.

کلید واژه: تهدید امنیتی، راهکارهای دفاعی، حمله.

فهرست مطالب

عنوان **صفحه**

مقدمه

۱-۱- مقدمه

در عصر ارتباطات، قدرت تکنولوژی و فناوری به عنوان یکی از منابع قدرت برای مقابله با تهدیدات فضای سایبری برای حکومتها و کشورها مطرح است. با توجه به تغییر ماهیت سنتی قدرت و امنیت و شکل گیری بعد جدیدی از تهدیدات برای کشورها، توجه به اینترنت و فضای سایبری، از ارکان اصلی سیاستگذاریها و تصمیم گیریها در درون دولتها تبدیل شده است و یا خواهد شد. جمهوری اسلامی ایران به عنوان یکی از کشورهای با موقعیت ژئوپولیتیکی مناسب در منطقه غرب آسیا، از تهدیدات فضای سایبری مبرا و جدا نیست. لذا توجه به توسعه و پیشرفت در حوزه فضای مجازی و سایبری، لازمه ادامه کشورداری و حکومتداری برای مسئولان است. یافته‌ها نشان می‌دهند که جمهوری اسلامی ایران از تهدیدات فضای سایبری مبرّا نیست و امنیت ملی کشور از طریق فضای سایبری مورد تهاجم قرار می‌گیرد و با مخاطراتی مواجه است که راهکارهای بدست آمده سبب توان افزایی امنیت ملی جمهوری اسلامی ایران از منظر ژئوپولیتیک خواهد شد.

۱-۲- امنیت سایبری چیست؟

امنیت سایبری یک مؤلفه مهم زیرساخت‌های شرکت است. موفقیت در توانایی یک شرکت به محافظت از اطلاعات اختصاصی و داده‌های مشتری در مقابل افرادی که سوء استفاده می‌کنند بستگی دارد. صرف نظر از اندازه، دامنه یا صنعت، هر شرکتی که می‌خواهد بقا داشته باشد باید ضمن ارزیابی خود، به دو سؤال اساسی پاسخ دهد:

- امنیت سایبری چیست؟
- چگونه یک استراتژی موفق در زمینه امنیت سایبری ایجاد کنیم؟

۱-۳- تعریف امنیت سایبری

امنیت سایبری شامل یک سری پروتکل است که یک شرکت یا یک فرد برای اطمینان از اطلاعات از ICA خود پیروی می‌کند. ICA مخفف کلمات یکپارچگی، محرمانه بودن و در دسترس بودن می‌باشد. اگر از امنیت مناسبی برخوردار باشید، می‌توانید خیلی سریع در مواقع قطعی برق، خطاها یا خرابی‌های هارد را

بازیابی کنید؛ زیرا این نوع حوادث باعث می‌شود که کارایی شما در برابر حملات خارجی و هکرها آسیب پذیرتر شود.

مفاهیم تداوم تجارت و بازیابی فاجعه، راهبردهای اساسی امنیت سایبری است. استمرار تجارت برای بقای یک تجارت ضروری است. بازیابی سریع تهدیدها به این معنی است که می‌توانید مخاطبان خود را در موقعیت‌های مشکل ساز حفظ کنید. بازیابی فاجعه به معنای حفظ تمامیت داده‌ها و زیرساخت‌های شما پس از یک رویداد فاجعه بار است. این تهدیدها در نهایت با سطح امنیت سایبری که در حال حاضر در زیرساخت‌های دیجیتالی شما اجرا می‌شود، طبقه بندی می‌شوند.

۱-٤- اهمیت امنیت سایبری

چرا باید امنیت در صدر برنامه‌های هر شرکت باشد؟ چرا باید مدیریت ارشد، خود را نسبت به امنیت سایبری نگران کند؟ یک دلیل غیرقابل انکار وجود دارد: دنیای دیجیتال که در آن تجارت می‌کنیم آسیب پذیر است و در معرض حمله سایبری قرار دارد.

شبکه جهانی هنوز باید راه طولانی را پیش از تبدیل شدن به یک اکوسیستم کاملاً امن که برای تنظیم و کنترل خود برنامه ریزی شده است، طی کند. تصمیم گیرندگان باید اطمینان حاصل کنند که کلیه سیستم‌های شرکت خود، از آخرین استانداردهای با امنیت بالا پیروی می‌کنند. کارمندان همچنین باید در پروتکل‌های اولیه امنیت سایبری آموزش ببینند. این به ویژه در مورد کارمندان غیر فناوری صادق است. به عنوان مثال، همه باید بدانند چگونه یک ایمیل فیشینگ صورت می‌پذیرد و چگونه باید از آن جلوگیری کرد.

بدون استراتژی امنیتی صحیح، ممکن است اتفاقات غیر قابل جبرانی رخ دهد. مهاجمان می‌دانند که چگونه نقاط ضعف را بیابند و از آنها بهره برداری کنند، شکاف‌هایی را باز می‌کنند که باعث می‌شود سیستم‌های قوی از بین بروند.

۱-۵- چالش‌های امنیت سایبری

بهترین استراتژی‌های امنیت سایبری فراتر از اصول ذکر شده در بالا است. هر هکر پیشرفته می‌تواند از این دفاع ساده عبور کند. با گسترش یک شرکت، امنیت سایبری نیز دشوارتر می‌شود.

۱-۶- گسترش فرصت‌های حمله برای هکرها

چالش دیگر امنیت سایبری، مقابله با همپوشانی فزاینده بین دنیای فیزیکی و مجازی مبادله اطلاعات است. هرچه اتومبیل‌های بدون راننده و سایر دستگاه‌های خود تنظیم شده رایج شوند، اینترنت اشیاء و سیاست های تجاریBYOD به مجرمان دسترسی بیشتری به سیستم‌های فیزیکی سایبر می‌دهد. این امر شامل ماشین‌ها، کارخانه‌ها، یخچال هوشمند و توستر در آشپزخانه شما، حتی برای یک دستگاه ضربان ساز پزشکی می‌باشد. در آینده، نفوذ به یکی از این سیستم‌ها ممکن است به معنای نفوذ به همه آن‌ها باشد.

۱-۷- مقررات پیچیده

محیط نظارتی همچنین امنیت سایبری را خصوصاً مباحث سیاسی پیرامون حفظ حریم شخصی کاربر، پیچیده می‌کند. اتحادیه اروپا به تازگی چارچوب تنظیم مقررات عمومی حفاظت از داده‌ها (GDPR) را به اجرا گذاشته است و موانع بیشتری را برای شرکت‌ها ایجاد می‌کند تا اطمینان حاصل کند که بدون انجام جریمه‌های سنگین تجارت کنند. دستورالعمل‌های امنیتی در موافقت نامه‌های نظارتی مانند GDPR باعث می‌شود که همه شرکت‌ها به یک استاندارد بالاتر نگاه داشته شوند که می‌تواند در کوتاه مدت به عوارض بیشتری برای SMB ها و نوآوری‌ها منجر شود. در دراز مدت، محیط مجازی احتمالاً برای همه افراد ایمن‌تر خواهد بود.

۱-۸- عدم تخصص فناوری اطلاعات

یک چالش مهم در امنیت سایبری عدم وجود متخصصان واجد شرایط برای انجام کار است. افراد زیادی در سطح پایین طیف امنیت سایبری با مهارت‌های عمومی قرار دارند. کارشناسان امنیتی که می‌دانند چگونه از شرکت‌ها در برابر هکرهای پیشرفته محافظت کنند، نادر هستند. کسانی که می‌دانند چگونه کارها را انجام دهند می‌دانند که چقدر این امر اهمیت دارد. فقط بزرگترین و ثروتمندترین شرکت‌های جهان می‌توانند از این خدمات سطح ویژه برخوردار شوند که همین موضوع مانعی دیگر است که SMB ها برای رقابت آنلاین باید بر آن غلبه کنند.

۱-۹- انواع امنیت سایبری

پوشش فضای مجازی موضوعی گسترده است. یک استراتژی جامع شامل همه این جنبه‌ها است و هیچکدام را نادیده نمی‌گیرد.

۱-۹-۱- زیرساخت‌های بحرانی

زیرساخت‌های مهم جهان به عنوان یک هیبرید سایبری-فیزیکی عمل می‌کند. همه چیز از بیمارستان‌ها گرفته تا کارخانه‌های تصفیه آب تا شبکه برق اکنون وارد دنیای آنلاین شده و دیجیتالی هستند. ما از این ساختار فوق العاده مزایای بسیاری کسب می‌کنیم. با این وجود، قرار دادن یک سیستم آنلاین، آسیب پذیری جدیدی را در برابر حملات سایبری و هک شدن ایجاد می‌کند. هنگامی که یک شرکت ابتدا خود را به دنیای فیزیکی و سپس دیجیتال متصل می‌کند، اولین زیرساختی که به آن وصل می‌شود، زیرساخت بحرانی است.

تصمیم گیرندگان شرکت باید این دیدگاه را در برنامه خود وارد کنند که چگونه حملات ممکن است بر عملکرد آن‌ها تأثیر بگذارد.

۱-۹-۲- امنیت شبکه

امنیت یک شبکه از یک شرکت در برابر دسترسی و نفوذ غیرمجاز محافظت می‌کند. امنیت مناسب بر روی یک شبکه همچنین می‌تواند تهدیدات داخلی برای سیستم را پیدا کرده و از بین ببرد.

اجرای مؤثر امنیت شبکه غالباً نیاز به برخی سازش و تجارت دارد. به عنوان مثال، ورود به سیستمی که دارای محافظت از اطلاعات است، از دسترسی غیرمجاز به اطلاعات جلوگیری می‌کند، اما همچنین باعث کاهش بهره وری شرکت می‌شود. یکی از مشکلات قابل توجه امنیت شبکه این است که از منابع زیادی استفاده می‌کند.

ابزارهای امنیتی شبکه مقادیر عظیمی از داده‌ها را تولید می‌کنند. حتی اگر یک سیستم امنیتی شبکه تهدیدی پیدا کند، ممکن است به دلیل حجم بالای داده‌هایی که تولید می‌شود، شکاف را از بین نبرد. تیم‌های فناوری اطلاعات اکنون در حال استفاده از یادگیری ماشین برای شناسایی خودکار تهدیدات امنیتی هستند که از این طریق خطای انسانی را کاهش می‌دهند.

۱-۹-۳- امنیت هاست ابری

امنیت ابر مجموعه‌ای از سیاست‌ها، کنترل‌ها و رویه‌ها است، همراه با فناوری‌هایی که برای محافظت از داده‌ها، زیرساخت‌ها و سیستم‌های مبتنی بر ابر کار می‌کنند.

به طور کلی اقدامات امنیتی خاصی هستند که برای محافظت از حریم خصوصی مشتری، داده‌ها، پشتیبانی از رعایت مقررات تنظیم می‌شوند و همچنین قوانین احراز هویت را برای دستگاه‌ها و کاربران

تنظیم می‌کنند. این اقدامات شامل هر رویدادی اعم از فیلتر کردن ترافیک، تأیید اعتبار برای دسترسی و پیکربندی امنیت ابری برای نیازهای خاص مشتری و ... می‌باشد.

۱-۹-٤- امنیت برنامه

بسیاری از بهترین هکرهای مدرن، امنیت برنامه‌های وب را ضعیف‌ترین نقطه برای حمله به یک سازمان می‌دانند. به دلیل گسترش روابط جدید با شرکت‌های برنامه‌هایی که هنوز صحت و اطمینان لازم را ندارند، نمی‌توانید با آن‌ها سر و کار داشته باشید. امنیت برنامه با رمزگذاری عالی شروع می‌شود که یافتن آن نیز چالش برانگیز است. پس از دستیابی به شیوه‌های رمزگذاری ایمن، آزمایش نفوذ و فازی دو روش امنیتی دیگر است که هم اکنون شرکت‌ها باید شروع به اجرای آن کنند.

۱-۹-٥- امنیت اینترنت اشیا

اینترنت اشیا یک سیستم مهم فیزیکی سایبر در ارتباط سیستم‌های آنلاین است. به طور خاص، اینترنت اشیا به سیستم دستگاه‌های محاسباتی درهم تنیده اشاره دارد که می‌تواند به عنوان ماشین‌های مکانیکی و دیجیتالی یا اشیاء، حیوانات یا افرادی تعریف شود که شناسه‌های منحصر به فرد به آنها داده می‌شود و در ظرفیت‌های مختلف، دیجیتالی می‌شوند. همچنین به توانایی مجزا این سیستم برای انتقال داده از طریق شبکه بدون نیاز به تعامل انسان به انسان یا انسان با کامپیوتر است.

اینترنت اشیاء کاربران را به روشی بی سابقه و بی نظیر به زیرساخت‌های مهم متصل می‌کند. امروزه، دستگاه‌های اینترنت اشیا اغلب در حالت ناامن به مصرف کنندگان ارسال می‌شوند. دستگاه‌های بسیاری نیز وجود دارند که هیچ گونه تدابیر امنیتی ندارند و همین امر باعث می‌شود اهداف اصلی بات نت‌ها باشند.

۱-۹-٦- تدوین استراتژی امنیت سایبری

هر استراتژی باید به صورت سفارشی طراحی شود. یک استراتژی امنیت سایبری که برای یک شرکت کار می‌کند، لزوماً برای دیگری مؤثر نخواهد بود. این امر برای هر موجودیت بسته به نیازها و آسیب پذیری های خاص آنها متفاوت است. با این حال، برخی از موضوعات اصلی وجود دارد که می‌توانید بدون توجه به اندازه، دامنه یا صنعت شرکت خود، آن‌ها را در نظر بگیرید.

۱-۹-۷- درک خطرات ناشی از عملکردهای مهم اقتصادی

امنیت سایبری دائماً پیچیده‌تر می‌شود. سازمان‌ها باید در مورد اینکه امنیت سایبری برای عملکردشان، دارای یک "دید امنیتی" باشند. این شامل ایجاد سطح قابل قبول از ریسک و اولویت بندی مناطق برای هدف قرار دادن اکثر سرمایه گذاری‌های امنیتی است.

۱-۹-۸- تلفیق استراتژی در بخش‌ها

یک استراتژی امنیتی خوب باید در کلیه اقدامات امنیتی که یک شرکت از قبل در آن قرار داده است، کار کند. شرکت‌ها برای بستن شکاف‌ها و بهبود امنیت کلی باید در مناطق حساس مداخله کنند.

۱-۹-۹- تهدیدات داخلی را از بین ببرید

بسیاری از پشت پرده‌ها و آسیب پذیری هایی که یک شرکت را به قربانی سایبری محکوم می‌کند از یک مشکل داخلی شروع می‌شود. بخشی از هر بسته امنیت سایبری باید شامل نظارت داخلی باشد تا از سوء استفاده شخصی افراد از دسترسی آن‌ها جلوگیری شود. نظارت محافظ کارانه همچنین به یک شرکت کمک می‌کند تا بین حملات خودی که هدفمند یا تصادفی هستند، تمایز قائل شود.

۱-۹-۱۰- برنامه ریزی های پیشگیرانه داشته باشید

درک کنید که هکرها همیشه یک قدم جلوتر از منحنی امنیت هستند. مهم نیست که دفاع شما چقدر خوب باشد، در بعضی مواقع نقض می‌شوند. معیارهای بازیابی کسب و کار خود را تقویت کنید تا وقتی اتفاقی رخ داد، بتوانید در اسرع وقت به عملکرد عادی برگردید.

با رعایت اصول امنیت سایبری، آیا یک شرکت اکنون باید با بینش جدید خود در مورد حفاظت اطلاعات، احساس آرامش کند؟ اصلاً. امنیت سایبری به معنای باقی ماندن هوشیارانه در اکوسیستم دیجیتال به صورت پویا است. راه حل‌هایی که امروز کار می‌کنند، فردا کارایی ندارند. تا آن زمان هکرها چیز دیگری را فهمیده‌اند و حتی با اعدام‌های بسیار قدرتمند در ورودی شما خواهند بود. در اینجا یک چک لیست امنیت سایبری برای شروع کار آمده است:

- سیاست‌ها و رویه‌ها را در جای خود قرار دهید.
- امنیت gatway را تضمین کنید.
- Security End Pointداشته باشید.
- پیاده سازی هویت و مدیریت دسترسی
- تأیید هویت چند عاملی
- محافظت از تحرک، دسترسی از راه دور و شبکه‌های خصوصی مجازی را بدست آورید.
- از امنیت شبکه بی سیم برخوردار باشید.
- تهیه نسخه پشتیبان و بازیابی فاجعه

- آموزش آگاهی از امنیت کارمندان را ارائه دهید.
- خطر امنیت سایبری خود را کاهش دهید.

فصل ۲– حمله سایبری و آشنایی با شایع‌ترین حملات سایبری

۲-۱- حملات سایبری چیست؟

حمله سایبری یک اقدام مخرب و آگاهانه توسط یک فرد یا سازمان برای نقض سیستم اطلاعاتی شخص یا سازمان دیگر است. معمولاً مهاجم به دنبال نوعی مزاحمت برای ایجاد اختلال در شبکه قربانی است.

حملات سایبری در لیست خطرات جهانی رتبه پنجم را در سال ۲۰۲۰ به خود اختصاص داده است و به یک قاعده جدید در بخش‌های دولتی و خصوصی تبدیل شده است. این صنعت پر خطر در سال ۲۰۲۱ همچنان در حال رشد است، زیرا انتظار می‌رود حملات سایبری اینترنت اشیا به تنهایی تا سال ۲۰۲۵ دو برابر شود.

اگر شما یکی از بسیاری از کسانی هستید که یک کسب و کار در حال رشد را تشکیل داده‌اید، می دانید که چشم انداز همیشه در حال تغییر است و حداقل سال ۲۰۲۰، تغییرات متعددی را ایجاد کرده است. بیماری همه گیر کرونا، همه نوع مشاغل، بزرگ و کوچک را تحت تأثیر قرار داده است.

جرائم اینترنتی که شامل سرقت یا اختلاس گرفته تا هک و تخریب داده‌ها می‌باشد، در نتیجه شیوع COVID-19حدود ۶۰۰٪ افزایش یافته است. تقریباً هر صنعتی مجبور شده است از راه حل‌های جدید استقبال کند.

۲-۲- حملات سایبری چند بار رخ می‌دهد؟

حمله سایبری یک اقدام مخرب و آگاهانه توسط یک فرد یا سازمان برای نقض سیستم اطلاعاتی شخص یا سازمان دیگر است. حملات سایبری هر روز به مشاغل آسیب می زند. این آسیب‌ها بعضی از مشاغل را از پای در می‌آورد و بعضی دیگر می‌توانند با تلاش به روال خود باز گردند.

دو نوع شرکت وجود دارند: **شرکت‌هایی که هک شده‌اند و کسانی که هنوز نمی‌دانند هک شده‌اند.**

۲-۳- تأثیر و شدت حملات سایبری

حملات سایبری می‌تواند از بسیاری جهات بر سازمان‌ها تأثیر بگذارد، از اختلالات جزئی در عملیات گرفته تا خسارات عمده مالی. صرف نظر از نوع حمله سایبری، هر نتیجه‌ای نوعی هزینه دارد چه پولی و چه غیر پولی.

پیامدهای حملات سایبری ممکن است هفته‌ها و یا ماه‌ها بعد بر روی کسب و کار شما تأثیر بگذارد. در ادامه پنج منطقه‌ای که ممکن است تجارت شما آسیب ببیند را لیست کرده‌ایم:

- خسارات مالی
- از دست دادن بهره وری
- خسارت به اعتبار شما
- مشکلات مداوم بیزینسی
- بدهی‌های قانونی

حملات باج افزار به عنوان یک نگرانی بزرگ شیوع بیشتری پیدا کرده است. در پایان سال ۲۰۱۶ هر ۴۰ ثانیه یک تجارت قربانی حمله باج افزار می‌شد. بر اساس گزارشی از Cybersecurity Ventures انتظار می‌رود این میزان تا امسال هر ۱۱ ثانیه افزایش یابد. این حمله سایبری زمانی اتفاق می افتد که از نرم افزار مخربی برای محدود کردن دسترسی به سیستم رایانه‌ای یا داده‌ها استفاده شود تا زمانی که قربانی باج خواسته شده توسط مجرم را پرداخت کند.

۲-٤- چرا افراد حملات سایبری را انجام می‌دهند؟

از زمانی که افراد از سیستم‌های تجاری آسیب پذیر بهره مند می‌شوند، جرائم سایبری افزایش یافته است. غالباً مهاجمان به دنبال باج گرفتن هستند: ۵۳ درصد از حملات سایبر منجر به خسارت ۵۰۰,۰۰۰ دلاری یا بیشتر شده است.

۲-۵- بات نت چیست؟

۵۳ درصد از حملات سایبر منجر به خسارت ۵۰۰۰۰۰ دلاری یا بیشتر شده است. بات نت شبکه‌ای از دستگاه‌های آلوده به نرم افزارهای مخرب مانند ویروس است. مهاجمان با هدف افزایش میزان حملات خود می‌توانند یک بات نت را به عنوان گروه کنترل کنند. غالباً از یک بات نت برای غلبه بر سیستم‌ها در یک حمله ی توزیع شده از انکار سرویس استفاده می‌شود.

۲-٦- انواع متداول حملات سایبری

حملات سایبری شامل انواع متداولی می‌باشد که در ادامه آن‌ها را بررسی می‌کنیم:

۲-۶-۱- بد افزار

بد افزار اصطلاحی است که برای توصیف نرم افزارهای مخرب از جمله نرم افزارهای جاسوسی، باج افزارها، ویروس‌ها و کرم‌ها به کار می‌رود. بدافزارها از طریق آسیب پذیری یک شبکه را نقض می‌کنند.

به طور معمول هنگامی که کاربر روی پیوند خطرناک یا پیوست نامه‌ای از طریق ایمیل کلیک می‌کند و سپس نرم افزار مخاطره آمیز را نصب می‌کند. پس از داخل شدن به سیستم، بدافزار می‌تواند موارد زیر را انجام دهد:

- دسترسی به مؤلفه‌های اصلی شبکه را مسدود می‌کند.
- بدافزار یا نرم افزار مضر اضافی را نصب می‌کند.
- به طور پنهانی با انتقال داده‌ها از هارد اطلاعات را به دست می‌آورد.
- برخی از مؤلفه‌ها را مختل کرده و سیستم را غیرقابل اجرا می‌کند.

بد افزار اصطلاحی است که برای توصیف نرم افزارهای مخرب از جمله نرم افزارهای جاسوسی، باج افزارها، ویروس‌ها و ... به کار می‌رود

۲-۶-۲- فیشینگ

فیشینگ عملی است که از طریق ارسال پیام‌های جعلی که به نظر می‌رسد از یک منبع معتبر می‌باشد، انجام می‌شود و معمولاً هم از طریق ایمیل اتفاق می افتد. هدف از این کار دزدی اطلاعات حساس مانند کارت اعتباری و اطلاعات ورود به سیستم یا نصب نرم افزارهای مخرب در دستگاه قربانی می‌باشد، فیشینگ یک شیوه رایج سایبری است.

۲-۶-۳- حمله مرد میانی

حملات مرد میانی که به عنوان حملات استراق سمع نیز شناخته می‌شوند، هنگامی اتفاق می افتد که مهاجمان خود را وارد معامله دو طرفه کنند، در واقع هکر از طریق شنود در بین دو دستگاهی که با یکدیگر تبادل داده می‌کنند قرار گرفته و بدون اطلاع سیستم قربانی، به اطلاعات محرمانه دسترسی پیدا می‌کند، به همین دلیل به عنوان حملات استراق سمع هم شناخته می‌شود.

هنگامی که مهاجمین ترافیک را قطع کردند، می‌توانند داده‌ها را فیلتر و سرقت کنند. مهاجم می‌تواند با ارسال کد مخرب در Query آسیب پذیر وب سایت، تزریق SQL را انجام دهد.

دو نقطه ورود مشترک برای حملات مرد میانیMitM:

- در Wi-Fi نا امن عمومی، مهاجمان می‌توانند خود را بین دستگاه بازدید کننده و شبکه قرار دهند و بدون اطلاع، بازدید کننده تمام اطلاعات را از طریق مهاجم منتقل می‌کند.
- هنگامی که بدافزار به دستگاهی رخنه کرد، یک مهاجم می‌تواند نرم افزاری را برای پردازش تمام اطلاعات قربانی نصب کند.

۲-٦-٤- تکذیب سرویس حمله

یک حمله تکذیب سرویس باعث می‌شود، سیستم‌ها، سرورها یا شبکه‌هایی را که دارای ترافیک برای خروج منابع و پهنای باند هستند، طغیان کنند. در نتیجه، سیستم قادر به انجام درخواست‌های مشروع نیست. مهاجمین همچنین می‌توانند از چندین دستگاه به خطر بیافتند تا این حمله را انجام دهند.

۲-٦-٥- تزریقSQL

تزریق ساختار هنگامی اتفاق می افتد که یک مهاجم کد مخرب را وارد سروری کند که از SQL استفاده می‌کند و سرور را مجبور می‌کند تا اطلاعاتی را که معمولاً وجود ندارد، فاش کند. یک مهاجم می‌تواند با ارسال کد مخرب در Query آسیب پذیر وب سایت، تزریق SQL را انجام دهد.

۲-٦-٦- بهره برداری از حمله روز صفر

پس از اعلام آسیب پذیری شبکه، یک بهره برداری صفر روز مشاهده می‌شود و در حقیقت پیش از آن که توسعه دهندگان بتوانند راه حلی برای آن بیابند، توسط مهاجمان استفاده شده و یا به اشتراک گذاشته می‌شود.

۲-۷- چگونه خطر حملات سایبری را کاهش دهیم؟

با افزایش تهدیدات هکرهایی که اطلاعات شما را نادرست کنترل می‌کنند، اجرای فرآیندهای جلوگیری از نقض امنیت داده بعد از داشتن بیمه حرفه‌ای و کافی برای نقض داده، از بهترین اقدامات است.

قوانین نقض داده‌ها در هر کشور متفاوت است، بنابراین بسته به محل کار شما، عوامل مختلفی باید در نظر گرفته شوند. نوتیفیکیشن های مربوط به این نقض، مواردی که تحت پوشش قرار گرفته‌اند و مجازات‌ها بسته به بروز و وضعیتی که در آن قرار دارید متفاوت خواهد بود؛ اما:

۲-۷-۱- انتقال داده‌ها را کاهش دهید

انتقال داده‌ها بین دستگاه‌های شخصی و بیزینسی، اغلب به دلیل افزایش روز افزون کارمندانی که از راه دور کار می‌کنند، اجتناب ناپذیر است. نگهداری اطلاعات حساس در دستگاه‌های شخصی آسیب پذیری در برابر حملات سایبری را به میزان قابل توجهی افزایش می‌دهد.

۲-۷-۲- با دقت دانلود کنید

دانلود فایل‌ها از منابع تأیید نشده می‌تواند سیستم‌ها و دستگاه‌های شما را در معرض خطرات امنیتی قرار دهد. برای کاهش حساسیت دستگاه خود در برابر بدافزار، مهم است که فقط فایل‌ها را از منابع معتبر دانلود کنید و از دانلودهای غیر ضروری خودداری کنید.

۲-۷-۳- امنیت رمز عبور را بهبود ببخشید

قدرت رمز عبور اولین خط دفاعی در برابر حملات مختلف است. با استفاده از ترکیبی از نمادها که معنی ندارند، تغییر رمز عبور به طور منظم و ذخیره نکردن آن یا به اشتراک گذاری آن، یک مرحله حیاتی برای محافظت از اطلاعات حساس شماست.

۲-۷-٤- سیستم عامل دستگاه خود را به روز کنید

ارائه دهندگان سیستم عامل دستگاه‌ها به سختی کار می‌کنند تا به طور مداوم سیستم عامل خود را ایمن‌تر کنند و نصب منظم آخرین به روزرسانی ها باعث آسیب پذیری کمتر دستگاه در برابر حملات می‌شود.

۲-۷-٥- نظارت بر نشت داده‌ها

نظارت منظم بر داده‌های شما و شناسایی نشت‌های موجود به کاهش تأثیر احتمالی نشت طولانی مدت داده‌ها کمک می‌کند. ابزارهای نظارت بر نقض داده‌ها فعالیت مشکوک را به طور فعال کنترل کرده و به شما هشدار می‌دهند.

۲-۷-٦- پلن پاسخ به نقض داده را ایجاد کنید

نقض داده حتی برای دقیق‌ترین و با نظم ترین شرکت‌ها نیز ممکن است اتفاق بیفتد. ایجاد یک برنامه رسمی برای مدیریت حوادث احتمالی به سازمان‌ها در هر اندازه‌ای کمک می‌کند تا در برابر حملات واقعی پاسخ دهند و آسیب‌های احتمالی آن‌ها را مهار کنند.

۲-۸- سوالاتی که ممکن است برایتان پیش بیاید

جنگ سایبری چیست؟

به نوعی از نبرد می گویند که طرفین از رایانه و شبکه استفاده می‌کنند تا جنگ را راه اندازی کنند.

امنیت سایبری چیست؟

شامل اقداماتی که برای محافظت از شبکه، داده‌ها و اطلاعات در مقابل تهدیدات داخلی و خارجی است.

فضای سایبری چیست؟

به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق کامپیوتر و مخابرات بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود.

آیا تا کنون به ایران حمله سایبری شده است؟

در ژوئن ۲۰۱۰ تاسیسات هسته‌ای ایران در نطنز توسط یک بدافزار مورد حمله سایبری واقع شد.

فصل ۳– امنیت سایبری چیست تأمین آن

۳-۱- فضای سایبری چیست؟

فضای سایبری به دنیایی مجازی گفته می‌شود که با متصل کردن کامپیوترها، دستگاه‌های با قابلیت اتصال به اینترنت، سرورها، روترها و سایر مولفه‌هایی که زیرساخت اینترنت را شکل می‌دهند پدید می‌آید. فضای مجازی، برخلاف خود اینترنت، موجودیتی است که توسط این پیوندها پدید می‌آید.

اصطلاح فضای مجازی اولین بار توسط ویلیام گیبسون نویسنده کانادایی آمریکایی در سال ۱۹۸۲ در داستانی که در مجله Omni منتشر شد و سپس در کتاب Neuromancer به شکل گسترده از آن استفاده شد رواج پیدا کرد. گیبسون در این رمان علمی تخیلی، فضای مجازی را برآیند شکل‌گیری شبکه‌ای رایانه‌ای در جهانی مملو از موجودات هوشمند مصنوعی تعبیر کرد.

در فرهنگ رایج دهه ۹۰ میلادی، فضای مجازی به عنوان یک اصطلاح کلی برای توصیف مکانی در نظر گرفته شد که مردم هنگام استفاده از اینترنت برای تعامل با یکدیگر از آن استفاده می‌کردند. این مکان محلی است که بازی‌های آنلاین در آن انجام می‌شود، اتاق‌های گفت‌وگو، پیام‌رسان‌های فوری و شبکه‌های اجتماعی در آن قرار دارند. اگر این نظریه را ملاک قرار دهیم، وب‌سایت‌های ارائه‌دهنده بازی‌های آنلاین، اتاق‌های گفت‌وگو و شبکه‌های اجتماعی منشأ شکل‌گیری این مفهوم هستند.

فضای مجازی با ظهور پدیده‌های نوظهور دیگری مثل شبکه‌های اجتماعی و وبلاگ‌ها در اواخر قرن بیست‌ویکم به مکانی مهم برای تبادل نظرهای عمومی، اجتماعی و سیاسی تبدیل شد. معمولاً بلاگ‌ها توسط افرادی ساخته می‌شوند که عقاید شخصی خود را می‌نویسند و غالباً به معرفی وب‌سایت‌هایی می‌پردازند که به آن‌ها علاقه دارند. با ظهور گسترده نرم‌افزارهای وبلاگ‌سازی، حتی افرادی که با توسعه وب آشنا نیستند موفق شدند وبلاگ‌های خود را ایجاد کنند.

۳-۲- مولفه‌های فضای سایبری

فضای مجازی یک دامنه جهانی در یک محیط اطلاعاتی متشکل از شبکه‌ها و زیرساخت‌های فناوری اطلاعات مثل اینترنت، شبکه‌های ارتباطی راه دور، سیستم‌های رایانه‌ای، پردازنده‌ها، کنترل‌کننده‌ها و... است. فضای مجازی را می‌توان در قالب سه لایه (فیزیکی، منطقی و اجتماعی) و متشکل از پنج مؤلفه (جغرافیایی، شبکه فیزیکی، شبکه منطقی، پرسونای سایبری و پرسونای کلی) توصیف کرد. توصیف هر یک از این مولفه‌ها به شرح زیر است:

۳-۲-۱- فیزیکی

لایه فیزیکی شامل مؤلفه جغرافیایی و شبکه فیزیکی است. مؤلفه جغرافیایی موقعیت فیزیکی عناصر شبکه را نشان می‌دهد. از منظر مؤلفه جغرافیایی جنبه‌های فیزیکی باید با یکدیگر در ارتباط باشند تا امکان تعامل با افرادی که در کشورها یا قاره‌های دیگر زندگی می‌کنند فراهم شود. مؤلفه شبکه فیزیکی، شامل تمامی سخت‌افزارها و زیرساخت‌هایی (سیمی، بی‌سیم و نوری) است که از شبکه و اتصالات فیزیکی (سیم، کابل، فرکانس رادیویی، روتر، سرور و رایانه) پشتیبانی می‌کند.

۳-۲-۲- منطقی

لایه منطقی شامل مؤلفه شبکه منطقی است که ماهیت فنی دارد و شامل اتصالات منطقی بین گره‌های شبکه است. به هر دستگاهی که به شبکه متصل باشند گره نام دارد مثل رایانه، دستیارهای شخصی دیجیتال، تلفن‌های همراه یا سایر وسایل شبکه. در شبکه مبتنی بر پروتکل اینترنت یک گره هر دستگاهی است که یک آدرس آی‌پی دارد.

۳-۲-۳- اجتماعی

لایه اجتماعی شامل جنبه‌های انسانی و شناختی است و شامل مؤلفه شخصیت سایبری و پرسونای واقعی افراد است. مؤلفه پرسونای سایبری شامل اطلاعاتی است که برای شناسایی یا تعیین هویت یک فرد در شبکه استفاده می‌شود آدرس ایمیل، آدرس آی‌پی رایانه، شماره تلفن همراه و سایر موارد. مؤلفه پرسونا به ماهیت واقعی افراد در شبکه اشاره دارد. یک فرد می‌تواند صاحب چند شخصیت سایبری باشد به عنوان مثال حساب‌های ایمیلی مختلف در رایانه‌های مختلف. پس یک شخص واقعی می‌تواند حساب‌های کاربری مختلفی در فضای سایبری داشته باشد.

فضای سایبری که روزانه به آن متصل می‌شوید متشکل از سه لایه اصلی است که تمامی مولفه‌ها، تجهیزات و تعاملات درون این سه لایه طبقه‌بندی می‌شوند.

۳-۳- اصطلاحات فضای سایبری

فضای سایبری متشکل از میلیاردها اصطلاح کوچک و بزرگی است که هر یک تعاریف و معنای خاص خود را دارند. با این‌حال برخی از آن‌ها کاربرد گسترده‌ای داشته و شناخته شده‌تر هستند. از مهم‌ترین اصطلاحات در این زمینه باید به اینترنت، آرپانت، زیرساخت ملی اطلاعات، W3، WWW، World Wide Web، فضای سایبری، شبکه اجتماعی، ابرفضا بزرگراه اطلاعات، شبکه آنلاین، ستون فقرات اینترنت، آیکان،

شبکه گسترده عریض مستندات فرامتن، سرور اطلاعات، وبلاگ، زبان‌های توسعه‌دهنده وب، هوش مصنوعی، محیط سه‌بعدی شبیه‌سازی شده، واقعیت افزوده، واقعیت مجازی و... اشاره کرد.

۳-٤- امنیت سایبری چیست؟

سازمان‌ها در زمان انجام فعالیت‌های تجاری، داده‌های حساس را از طریق شبکه‌ها و سایر دستگاه‌ها منتقل می‌کنند و درست در همین نقطه است که امنیت سایبری با ارائه مجموعه‌ای متشکل از راه‌حل‌های سخت‌افزاری و نرم‌افزاری به محافظت از این اطلاعات و سیستم‌های پردازش یا ذخیره اطلاعات می‌پردازد.

با افزایش حجم و پیچیدگی حملات سایبری، شرکت‌ها و سازمان‌ها به ویژه آن‌هایی که وظیفه حفاظت از اطلاعات مربوط به امنیت ملی، بهداشتی یا سوابق مالی را بر عهده دارند باید اقدامات لازم برای محافظت از اطلاعات حساس را انجام دهند. سال گذشته میلادی بود که شرکت‌های امنیتی هشدار دادند حملات سایبری و جاسوسی دیجیتال مهم‌ترین تهدید برای امنیت کشورها هستند و حتا از اصطلاح تروریسم برای خطرناک بودن این تهدیدات استفاده کردند.

امنیت سایبری یعنی محافظت از سیستم‌ها، شبکه‌ها و برنامه‌ها در برابر حملات دیجیتالی. دسترسی، تغییر و نابودی اطلاعات مهم، دریافت پول از کاربران و ایجاد وقفه در روال کسب‌وکارها از اهداف حملات سایبری است. پیاده سازی امنیت سایبری به صورت مؤثر و درست، از چالش‌های دنیای امروز است چون هم تعداد دستگاه‌ها بیشتر شده و هم هکرها خلاق‌تر شده‌اند. امنیت سایبری، کامپیوترها، سرورها، موبایل‌ها و سیستم‌های الکترونیکی را از حملات شرورانه حفظ می‌کند و وظیفه آن در سه مورد زیر خلاصه می‌شود:

۱. حفاظت از دستگاه‌هایی که افراد استفاده می‌کنند.
۲. حفاظت از اطلاعاتی که روی این دستگاه‌ها قرار دارند.
۳. . حفاظت از هویت افرادی که از این اطلاعات استفاده می‌کنند.

۳-۵- اهمیت امنیت سایبری

تهدیدات سایبری با سرعت زیادی رشد می‌کند و هر ساله تعداد رخنه‌ها در حال افزایش است. ۷.۹ میلیارد ثبت رخنه تنها در نه ماه اول سال ۲۰۱۹ انجام شده که در مقایسه با همین مدت در سال ۲۰۱۸، بیش از دو برابر (۱۱۲٪) شده است. بیشتر رخنه‌ها در سرویس‌های پزشکی و سرویس‌های عمومی است. جرائم سایبری بیشتر به دنبال اطلاعات پزشکی و مالی است اما کسب‌وکارهایی که از شبکه‌ها استفاده می‌کنند هم هدف قرار می‌گیرند تا به اطلاعات مشتری و شرکت دست یابند یا به مشتری حمله شود.

پیش‌بینی شده تا سال ۲۰۲۲ حدود ۱۳۴ میلیارد دلار باید صرف امنیت سایبری شود. مسئول هدایت سازمان‌ها برای پیاده سازی مناسب امنیت سایبری در برابر حملات سایبری در سراسر دنیا، دولت‌ها هستند. با انجام چند کار ساده اما به موقع می‌تواند جلوی ضررهای بیشتر را گرفت. امنیت سایبری با همین هدف باید در صدر برنامه‌هایمان قرار گیرد. چه کسب‌وکار بزرگ داشته باشیم چه کاربر خانگی باشیم که اطلاعات شخصی مثل عکس و فیلم دارد. در زمینه امنیت سایبری باید برنامه مشخص و مدونی داشته باشیم.

در زمینه امنیت، گاهی بدون در نظر گرفتن پیامدهای منفی و طولانی مدت، تصمیمات نامناسبی می‌گیریم. افراد باهوش معمولاً کارهای غیرعاقلانه‌ای انجام می‌دهند. لیست بلندبالایی از کارهایی که باید انجام شود، برنامه‌های فشرده و بودجه کمی که در اختیار است، باعث می‌شود بدون در نظر گرفتن پیامدهای منفی و طولانی مدت آن، تصمیمات نامناسبی بگیریم.

امنیت سایبری از این جهت مهم است که سازمان‌های دولتی، نظامی، شرکتی، مالی و پزشکی حجم گسترده‌ای از اطلاعات را در رایانه‌ها و سایر دستگاه‌ها جمع‌آوری، پردازش و ذخیره می‌کنند. بخش قابل توجهی از این داده‌ها می‌توانند اطلاعات حساسی باشند مثل مالکیت معنوی، داده‌های مالی، اطلاعات شخصی یا انواع دیگر داده‌هایی که دسترسی غیر مجاز به آن‌ها یا افشای آن‌ها ضررهای جبران‌ناپذیری به افراد یا سازمان‌ها وارد می‌کند.

۳-۶- اهداف امنیت سایبری

هدف امنیت سایبری محافظت از اطلاعات در برابر سرقت و آسیب است. این اطلاعات شامل داده‌های حساس، اطلاعات قابل شناسایی و تشخیص هویت افراد، سوابق پزشکی، اطلاعات شخصی، مالکیت معنوی، داده‌های مرتبط با فعالیت آژانس‌های دولتی و صنعتی می‌شود.

بدون وجود امنیت سایبری، سازمان‌ها نمی‌توانند از خود در برابر نقض‌های داده‌ای نقض داده‌ای Data Breach به رویکردی اشاره دارد که باعث افشای داده‌های شخصی کاربران شده و به هکرها اجازه سوء استفاده از اطلاعات و جعل هویت افراد را می‌دهد. و حمله‌های هکری دفاع کنند و به هدفی ساده برای مجرمان سایبری تبدیل می‌شوند. مخاطرات امنیتی به دلیل گسترده‌تر شدن ارتباطات در مقیاس جهانی و استفاده از سرویس‌های ابری برای ذخیره‌سازی اطلاعات حساس و شخصی رو به افزایش است.

پیکربندی غیر اصولی خدمات ابری باعث شده تا حمله‌های سایبری شکل پیچیده‌ای به خود بگیرند. هر سازمانی ممکن است قربانی یک حمله سایبری موفق شده و با مشکل نقض داده‌ای در مقیاس کلان روبرو شود. روزهایی که دیوارهای آتش ساده و نرم‌افزارهای ضد ویروس تنها راهکارهای امنیتی مؤثر بودند سپری

شده و کارشناسان امنیتی نمی‌توانند همچون گذشته به مقابله با تهدیدات سایبری بپردازند و این تهدیدات می‌توانند از زوایای مختلفی به سازمان‌ها آسیب زنند.

امنیت سایبری با رویکردهای فنی و آموزشی به مقابله با چالش‌های امنیتی می‌پردازد مثلاً کارمندان درباره کلاهبرداری‌های ساده‌ای مثل مهندسی اجتماعی (فیشینگ) و حملات پیچیده‌تر مثل حملات باج افزاری، بدافزارهایی که برای سرقت مالکیت معنوی یا داده‌های شخصی طراحی شده‌اند آموزش‌های لازم را می‌بینند.

امنیت سایبری دیگر مفهومی نیست که کسب‌وکارها به سادگی از آن چشم‌پوشی کنند. حوادث امنیتی به‌طور منظم بر عملکرد مشاغل مختلف در هر اندازه‌ای تأثیرگذار است و اغلب به اعتبار یک شرکت خدشه وارد می‌کند.

۳-۷- انواع تهدیدات سایبری

تهدیدات در برابر امنیت سایبری به سه دسته تقسیم می‌شود:

۳-۷-۱- جرائم سایبری[1]

عبارت است از فرد یا گروهی که سیستم‌ها را هدف قرار می‌دهند تا درآمد کسب کنند یا خرابکاری کنند.

۳-۷-۲- حمله سایبری

Cyber Attack اغلب با هدف جمع‌آوری هدفمند اطلاعات، با انگیزه سیاسی است.

۳-۷-۳- تروریست سایبری

Cyber Terrorisom: با هدف ایجاد رعب و وحشت با خراب کردن سیستم‌های الکترونیکی است. اما برسیم به این مبحث که شرورهای سایبری چگونه کنترل سیستم‌های کامپیوتری را به دست می‌گیرند. رایج‌ترین روش‌ها برای تهدید امنیت سایبری عبارتند از:

.SQL injectionبرای آشنایی بیشتر با این روش هک که sql را نشانه می‌گیرد

- Phishing
- Man-in-the-middle attack

[1] CyberCrime

- Denial-of-service attack
- Social engineering

Dridex malwareو Romance scams و Emotet malware از جدیدترین روش‌های تهدیدات سایبری هستند که در امریکا، انگلیس و استرالیا گزارش شده است. تهدیدات فضای سایبری با در نظر گرفتن تمامی بردارهای حمله‌ای که کاربران، تجهیزات و شبکه‌ها را نشانه می‌روند، به صورت زیر دسته‌بندی می‌شوند:

۳-۷-٤- تهدیدات شبکه‌ها

کاربران، تجهیزات و کانال‌های ارتباطی در معرض انواع مختلفی از تهدیدات سایبری نظیر نفوذ، حمله انکار سرویسDoS، حمله انکار سرویس توزیع شدهDDoS، دوقلوهای شیطانی، حمله مرد میانی، حمله سیلابی، بات‌نت‌ها، ویروس‌ها، باج‌افزارها و... قرار دارند.

۳-۷-٥- تهدیدات برنامه‌های کاربردی

تمامی برنامه‌های کاربردی از سامانه‌های مدیریت بانک‌های اطلاعاتی گرفته تا برنامه‌های دسکتاپ، موبایل و سرور ممکن است به آسیب‌پذیری‌هایی آلوده باشند که به هکرها اجازه می‌دهند به واسطه آن‌ها به سامانه‌ها حمله کنند. به‌طور مثال، هکرها می‌توانند از خطای سرریز بافر برای تغییر کدها و روال اجرای یک برنامه استفاده کرده و با آلوده‌سازی حافظه اصلی به کدهای مخرب موقت، راه را برای ورود بدافزارها به سامانه‌ها هموار کنند، به همین دلیل برنامه‌ها برای اطمینان از ایمن بودن در برابر حملات نیازمند به‌روزرسانی و آزمایش مداوم هستند.

۳-۷-٦- تهدیدات نقاط پایانی

دسترسی از راه دور یکی از ارکان اجتناب‌ناپذیر کسب‌وکارهای امروزی است. همین مسئله شکاف امنیتی بزرگی به وجود می‌آورد که در نهایت نقض داده‌ای را باعث می‌شود. در این بردار حمله تمرکز هکرها روی کارمندانی است که از منازل خود و از طریق لپ‌تاپ‌های شخصی به شبکه سازمانی متصل می‌شوند. در این بردار حمله هکرها می‌توانند رمز عبور و نام حساب کاربری یک کارمند را سرقت کرده و به شکل مشروع به شبکه سازمانی نفوذ کنند.

۳-۷-۷- تهدیدات دستکاری داده‌ها

گاهی اوقات حمله‌های هکری با هدف دستکاری اطلاعات درون پایگاه‌های داده‌ای انجام می‌شوند. در این بردار حمله هکرها سعی می‌کنند ابتدا با روبایش یک حساب کاربری به شبکه سازمانی نفوذ کرده، سطح مجوزهای خود را ارتقا داده (مدیر شبکه، مدیر پایگاه داده یا توسعه‌دهنده پایگاه داده) و در ادامه به ویرایش

اطلاعات درون پایگاه‌های داده‌ای و نسخه‌های پشتیبان بپردازند. به همین دلیل بهتر است از لایه‌های امنیتی چندگانه برای محافظت از اطلاعات شرکت و مشتریان استفاده شود.

۳-۷-۸- تهدیدات هویت

این بردار حمله ارتباط مستقیمی با حمله فیشینگ دارد. در این حمله سعی می‌شود اطلاعات هویتی مدیرعامل اجرایی یا سایر مدیران اجرایی ارشد سازمان جعل شود و ایمیل‌هایی با هدف دسترسی به رمزهای عبور، انتقال وجه یا دسترسی به منابع از کارمندان واحدهای مربوطه دریافت شود.

۳-۷-۹- تهدیدات پایگاه‌های داده و زیرساخت‌ها

تمامی شبکه‌های ارتباطی بزرگ بر پایه تجهیزات فیزیکی و پایگاه‌های داده کار می‌کنند. یک حمله موفق به سوییچ یا روتری که آلوده به آسیب‌پذیری است یا تنظیمات آن به درستی پیکربندی نشده‌اند دسترسی نامحدود به منابع را فراهم می‌کند. در بردار حمله به زیرساخت‌ها هکرها سعی می‌کنند با آلوده‌سازی تجهیزات مهم مثل سرورها برای اهداف مختلفی نظیر استخراج رمز ارز از آن‌ها استفاده کنند.

۳-۷-۱۰- تهدیدات تجهیزات همراه

تلفن‌های همراه و تبلت‌ها ایده‌آل‌ترین ابزارها برای شنود و نفوذ به شبکه‌های سازمانی هستند. کافی است تنها یک کارمند سازمان بزرگی متقاعد شود تا بدافزاری را روی گوشی خود نصب کند تا به تنهایی هر نوع چالش امنیتی را برای سازمان رقم بزند.

۳-۸- انواع امنیت سایبری

گزارش‌ها حاکی از آن است که تا پایان سال ۲۰۲۱ حمله‌های سایبری حدود ۶ میلیون دلار به اقتصاد جهانی آسیب وارد می‌کنند. بر همین اساس راه‌حل‌های امنیتی مختلفی در دسترس شرکت‌ها قرار دارد که همگی در زیرمجموعه‌های زیر طبقه‌بندی می‌شوند:

امنیت زیرساخت‌های حیاتی: تأمین امنیت سایبری زیرساخت‌های حیاتی به معنای محافظت از شبکه‌های ارتباطی، شبکه انتقال انرژی، تصفیه آب، چراغ‌های راهنمایی، پایانه‌های فروش و مراکز بهداشتی است. این مراکز ممکن است به‌طور مستقیم با حمله‌های سایبری مرتبط نباشند، اما می‌توانند به عنوان بستری برای ورود بدافزارها به نقاط پایانی سامانه‌هایی که به آن‌ها متصل می‌شوند استفاده شوند.

امنیت شبکه: امنیت شبکه از شبکه کامپیوتری در برابر اختلالگران محافظت می‌کند حال این اختلال می‌تواند بدافزار باشد و یا هک. امنیت شبکه مجموعه راهکارهایی است که سازمان‌ها را قادر می‌سازد تا

شبکه‌های رایانه‌ای را از دسترس افراد متجاوز، مهاجمان سازمان یافته و بدافزارها دور نگه دارند. به‌طور مثال، سازمان‌ها برای رشد تجاری از کوکی‌های شخص ثالث برای ردیابی فعالیت‌های کاربران استفاده می‌کنند، اما گاهی اوقات مشتریان قربانی این مسئله می‌شوند. از این‌رو برای مقابله با حملات سایبری و بدافزارهای مرتبط با شبکه باید موارد زیر را انجام دهید:

- برنامه امنیتی نظارت بر شبکه داخلی و زیرساخت‌ها را به کار گیرید و از فناوری‌های نوین مثل یادگیری ماشین برای بررسی ترافیک غیر عادی شبکه استفاده کنید.
- برای بهبود امنیت شبکه لاگین‌های اضافی را محدود کنید.
- برنامه تعویض منظم رمزهای عبور را تدوین کنید.
- برنامه‌های ضد ویروس قدرتمند نصب کنید.
- دیوارهای آتش را به درستی پیکربندی کنید.
- دسترس میهمان یا ناشناس را محدود کنید.
- ترافیک ورودی از اینترنت را ارزیابی کنید.
- از رمزگذاری برای محافظت از اطلاعات استفاده کنید.

۳-۸-۱- بهبود امنیت با اتکا به ابر

بیشتر سازمان‌ها به دنبال استفاده از هوش مصنوعی برای بهبود مشاغل خود، افزایش تجربه مشتری و بهبود عملکردها هستند. با وجود حجم انبوهی از داده‌های تولید شده توسط بخش‌های مختلف یک سازمان که اغلب فاقد ساختار و توسط منابع مختلف تولید می‌شوند، شبکه‌های سازمانی با تهدید بالقوه روبرو هستند. از این‌رو، شرکت‌های فعال در زمینه خدمات ابری با پیاده‌سازی راهکارهای امنیتی بالقوه به سازمان‌ها اجازه می‌دهند این حجم عظیم از داده‌های مستعد چالش‌های امنیتی را در فضای خارج از شبکه سازمانی ذخیره‌سازی و مدیریت کنند.

۳-۸-۲- امنیت با چاشنی اینترنت اشیا

یکی دیگر از راهکارهای نوین امنیتی، برخواسته از دل اینترنت اشیا است که تا پایان سال ۲۰۲۱ بازاری به ارزش ۵۲۰ میلیارد دلار خواهد داشت. تجهیزات و حس‌گرهای هوشمند در تعامل با اکوسیستم اینترنت اشیا می‌توانند از تجهیزات تجاری به بهترین شکل محافظت کنند، زیرا با ارائه اطلاعات لحظه‌ای گزارش دقیقی درباره عملکرد تجهیزات در اختیار شرکت‌ها قرار می‌دهند.

۳-۸-۳- بهبود امنیت با اتکا به برنامه‌های امنیتی

کاربران شیفته برنامه‌های مختلفی هستند که سهولت در انجام کارها را به ارمغان می‌آورند. برنامه‌های کاربردی نیز همانند شبکه‌های ارتباطی مستعد حمله‌های سایبری است، پس مهم است از راه‌حل‌های نرم‌افزاری و سخت‌افزاری نظیر سامانه‌های تشخیص نفوذ، سامانه‌های پیشگیری از نفوذ، دیوارهای آتش، ضدویروس‌ها و هانی‌پات‌ها و ضدبدافزارها برای محافظت از برنامه‌های کاربردی استفاده کنید.

۳-۸-٤- تدوین برنامه بازیابی پس از فاجعه

در صورت بروز یک حمله سایبری بهتر است از برنامه بازیابی پس از فاجعه برای بازگرداندن اطلاعات سالم استفاده کنید تا کسب‌وکارتان تداوم پیدا کند. برای این منظور به برنامه جامعی نیاز دارید که توسط کارشناسان امنیتی تدوین شده باشد. Disaster recovery و استمرار کسب‌وکار مشخص می‌کنند سازمان چگونه به از دست رفتن دیتا پاسخ می‌دهد. سیاست Disaster Recovery مشخص می‌کند چگونه اطلاعات پس از وقوع حادثه، به حالت قبل ری‌استور شوند. استمرار کسب‌وکار، برنامه سازمان برای بازگشت به شرایط عادی پس از وقوع حوادثی مانند سیل و زلزله است.

۳-۸-٥- امنیت اپلیکیشن

روی نگهداری نرم افزار و دستگاه‌ها تمرکز دارد. قبل از پیاده سازی دستگاه یا برنامه باید زمینه امنیت آن را تأمین کرد.

۳-۸-٦- امنیت اطلاعاتی

از یکپارچگی و حریم خصوصی دیتا محافظت می‌کند. این کار هم در رسانه ذخیره سازی و هم هنگام انتقال اطلاعات انجام می‌شود. شامل پروسه‌ها و تصمیماتی است که برای کنترل و حفاظت از دیتا انجام می‌شود. مثلاً Permission های کاربر هنگام دسترسی به شبکه و یا فرآیندهایی که مشخص می‌کنند اطلاعات چه موقع و کجا ممکن است ذخیره یا به اشتراک گذاشته شوند.

۳-۸-۷- آموزش کاربر

به مواردی غیرقابل پیش‌بینی امنیت سایبری اشاره می‌کند یعنی افراد. هر کسی ممکن است به طور تصادفی ویروسی وارد سیستم امنیتی کند. آموزش کاربر برای حذف پیوست‌های مشکوک در ایمیل، وصل نشدن به USB های ناشناس و دیگر موارد مهمی که حیاتی است باید جزو برنامه امینت سازمانی هر شرکتی باشد.

۳-۹- تأمین امنیت کاربر

بسیاری از شرکت‌ها فقط آنتی‌ویروسی را خریده و نصب می‌کنند با این تصور که برای حفاظت از آن‌ها کافیست. با وجودی که این کار اهمیت دارد، اما اصلاً کافی نیست. در دنیایی که افراد و سازمان‌هایی هستند که سعی در دزدیدن اطلاعات شما دارند، باید از چندین سطوح امنیتی استفاده کنید که هم شامل نرم افزار می‌شود و هم سخت افزار. باید از رمزگذاری داده و پسوردهای قوی که کاربران نتوانند آن را غیرفعال کنند نیز استفاده شود. حفاظت آر کاربر و امنیتEndpoint، قسمت مهمی از امنیت سایبری است. این کاربر نهایی است که ممکن است باموبایل و دسکتاپ و لپ تاپ، به طور تصادفی بدافزار یا هر شکلی از تهدید سایبری را آپلود کند.

امنیت سایبری برای تأمین امنیت کاربر از پروتکل‌های رمزنگاری استفاده می‌کند تا ایمیل‌ها، فایل‌ها و دیگر اطلاعات را رمزگذاری کند. این جفاظت تنها در انتقال دیتا نیست بلکه در برابر گم شدن و دزدیده شدن اطلاعات هم هست. نرم افزارهای امنیتی، کامپیوترهای کاربر را اسکن می‌کنند تا کدهای مشکوک را پیدا و حذف کنند. برنامه‌های امنیتی حتی می‌توانند کدهای خرابکار مخفی در Primary Boot Record را تشخیص داده و حذف کنند و طوری طراحی شده‌اند که دیتا را روی هارد درایو رمزگذاری کنند.

پروتکل‌های امنیت الکترونیکی روی تشخیص بلادرنگ تشخیص بدافزار تمرکز دارد. بسیاری از آنها از آنالیز رفتاری و سابقه استفاده می‌کنند تا رفتار یک برنامه را مانیتور کنند و با کدهایشان در برابر ویروس‌ها و تروژان‌ها مقابله کنند. برنامه‌های امنیتی با یادگیری رفتار کاربر می‌توانند آلودگی را تشخیص دهند.

۳-۱۰- مهم‌ترین نکات امنیت سایبری

نشت داده‌هایی که می‌توانند منجر به سرقت هویت و افشای اطلاعات حساس در مکان‌های عمومی مثل شبکه‌های اجتماعی شوند رو به افزایش است. اطلاعات حساس مانند شماره‌های تأمین اجتماعی، اطلاعات کارت اعتباری و جزئیات حساب بانکی ممکن است در سرویس‌های ذخیره‌ساز ابری مانند دارپ‌باکس یا گوگل درایو ذخیره شوند.

واقعیت این است که تمامی کاربران فضای سایبری برای انجام فعالیت‌های روزمره از سیستم‌های کامپیوتری استفاده کرده و به آن‌ها اعتماد می‌کنند. همین مسئله باعث شده تا وابستگی ما به سرویس‌های ابری بیشتر شود، در حالی که ضعف‌های مستتر در سرویس‌های ابری، تلفن‌های هوشمند و اینترنت اشیا به درستی شناسایی نشوند. به همین دلیل مهم است که تفاوت میان امنیت سایبری و امنیت اطلاعات را درک کنیم، حتی اگر مهارت‌های فنی این دو اصطلاح به یکدیگر شبیه باشند.

GDPR مثال عالی در این زمینه است که سازمان‌هایی که در اتحادیه اروپا به فعالیت اشتغال دارند را ملزم کرد از قوانین سفت و سخت اتحادیه اروپا پیروی کنند، رویکردی که موفق شده به میزان قابل توجهی مانع نقض‌های داده‌ای شود. از مهم‌ترین نکات امنیت سایبری که باید دقت ویژه‌ای به آن‌ها داشته باشید به موارد زیر باید اشاره کرد:

۱. نقض داده‌ای را اعلام کنید.

۲. کارشناس امنیت برای محافظت از اطلاعات استخدام کنید.

۳. برای کاربردهای تجاری که نیازمند داده‌های کاربران هستند از آن‌ها کسب اجازه کنید.

٤. داده‌ها را برای حفظ حریم خصوصی افراد ناشناس کنید.

٥. اطلاعات را به شکل عمومی افشا نکنید تا مجبور به پاسخ‌گویی به نهادهای قانونی نشوید.

٦. در صورت نقص داده‌ای در اسرع وقت به مقامات مربوطه گزارش دهید.

۷. تمام سطوح سازمان را در مورد خطرات مهندسی اجتماعی و کلاهبرداری‌های رایج مهندسی اجتماعی مانند ایمیل‌های فیشینگ و اشتباه تایپی [1]و حمله جعل آدرس اینترنتی [2]آگاه کنید.

۸. روی خرید و به‌کارگیری ابزارهایی که دسترسی به اطلاعات را محدود می‌کنند سرمایه‌گذاری کنید، دسترسی افراد ثالث یا پیمانکاران به اطلاعات سازمانی را محدود کنید و به‌طور مداوم دستگاه‌ها، پایگاه‌های داده و اطلاعاتی که با خطر نشتی روبرو هستند را اسکن کنید.

۹. از گذرواژه‌های پیچیده و طولانی همراه با احراز هویت دو عاملی یا چند عاملی برای ایمن‌سازی دسترسی به حساب‌های کاربری استفاده کنید. با توجه به این‌که در مکانیزم احراز هویت دو یا چند عاملی از لایه‌های امنیتی مختلفی برای ایمن‌سازی دسترسی به حساب‌ها استفاده می‌شود، اگر هکری بتواند رمز ورود به حساب کاربری را به‌طور دقیق حدس بزند، هنوز یک مرحله امنیتی اضافی برای تصاحب حساب کاربری پیش رو دارد.

۱۰. بهتر است از مکانیزم‌های ارتباطی ایمن مثل شبکه خصوصی مجازی برای اتصال به شبکه سازمانی استفاده کنید. این‌کار مانع از آن می‌شود تا هکرها بتوانند با سهولت حمله‌های مرد میانی را پیاده‌سازی کنند.

۱۱. بهتر است برای اتصال به شبکه‌های سازمانی یا ارسال اطلاعات حساس از وای‌فای عمومی استفاده نکنید، زیرا این احتمال وجود دارد که هکری قادر به شنود اطلاعات باشد.

[1] Typosquatting
[2] URL Hijacking

۱۲. نرم افزارها و سیستم عامل خود را آپدیت کنید. بهتر است از جدیدترین وصله‌ها Patch استفاده کنید.

۱۳. از نرم افزار آنتی ویروس استفاده کنید. این راهکار امنیتی، تهدیدات را تشخیص می‌دهند و پاک می‌کنند. به یاد داشته باشید همواره آنتی ویروس را آپدیت نگه دارید.

۱٤. پیوست ایمیل‌های دریافتی از فرستنده ناشناس را باز نکنید چون ممکن است بدافزار داشته باشند.

۱۵. روی لینک‌های موجود در ایمیل که از فرستنده ناشناس یا وب‌سایتِ ناآشنا است کلیک نکنید.

۳-۱۱- پروکسی‌های گمنام[1]

کاربران را قادر می‌سازد تا فعالیت‌های مرورگر خود را پنهان کنند. از آن‌ها اغلب برای دور زدن فیلترهای امنیت وب استفاده می‌شود. پروکسی‌های گمنام خطراتی جدی برای سازمان‌ها به همراه دارند:

۳-۱۱-۱- امنیت

پروکسی‌های گمنام تدابیر امنیتی وب را دور می‌زنند و کاربران را قادر می‌سازند تا به صفحات وب آلوده دسترسی پیدا کنند.

۳-۱۱-۲- مسئولیت قانون

اگر از کامپیوترهای سازمان برای مشاهده سایت‌های غیراخلاقی، فعالیت‌های کینه توزانه و یا ترغیب رفتارهای غیرقانونی استفاده شود ممکن است سازمان از لحاظ قانونی به دردسر بیافتد. همچنین رعایت نکردن لاینس‌های نرم‌افزاری شرکت‌های دیگر از طریق دانلودهای غیرقانونی فیلم، ترانه‌ها و نرم‌افزارها پیامدهای جدی به همراه دارد.

۳-۱۱-۳- بازدهی

پروکسی‌های گمنام می‌توانند به کاربران اجازه دهند تا به سایت‌هایی که اگر چه امن هستند ولی کاربری کاری ندارند دسترسی داشته باشند.

[1] Anonymizing Proxy

۳-۱۲- ویروس اتوران[1]

ویروس اتوران بدافزارهایی هستند که از ویژگی‌های اتوران ویندوز استفاده می‌کنند. ویژگی اتوران یکی از قابلیت‌هایی بود که سازندگان سیستم عامل جهت ایجاد تجربه‌ای لذت بخش برای کاربران فراهم نمودند تا نرم‌افزارها بتوانند بدون دخالت کاربر اجرا گردند؛ اما متاسفانه سازندگان بدافزار با سواستفاده از این قابلیت، آن را به یک تهدید تبدیل نمدند. هنگامی که دستگاه حاوی این گونه بدافزارها به کامپیوتر متصل می‌شوند بدافزارها به طور خودکار اجرا شده و باعث آلودگی رایانه می‌گردد.

ویروس ویروس اتوران معمولاً روی درایوهای USB بارگذاری می‌شوند و به محض اتصال به کامپیوتر آنها را آلوده می‌کنند. AutoPlay نیز فناوری مشابهی با اتوران دارد. این برنامه روی رسانه‌های قابل حمل اجرا می‌شود و کاربران را وادار می‌کند که برای گوش دادن به موسیقی از پخش‌کننده پیش‌فرض استفاده کنند و یا دیسک را در Windows Explorer باز کنند. مهاجمان از AutoPlay بهره می‌جویند و معروف‌ترین دستاورد آنها در این زمینه کرم Conficker است.

در نسخه‌های جدید سیستم‌عامل ویندوز، مایکروسافت به صورت پیش‌فرض اتوران را خاموش کرده و آن را در حالت خاموش قرار داده است. در نتیجه ویروس اتوران در آینده باعث تهدیدات کمتری خواهند بود.

[1] AutoRun Virus

فصل ۴– بهترین راه بک آپ گرفتن از اطلاعات کامپیوتر

٤-١- روش‌های بک آپ گرفتن از کامپیوتر و هارد اکسترنال با چند روش مختلف

اکثر ما تجربه از دست دادن داده‌ها و اطلاعاتمان را داریم. ممکن است همین فردا هارد دیسک کامپیوترتان دچار نقص شود، یک باج‌افزار فایل‌های شما را قفل کند یا یک خطای نرم‌افزاری باعث از بین رفتن فایل‌های مهم شما شود. در صورت عدم بک آپ گرفتن به صورت دائم و منظم از کامپیوترتان، این احتمال وجود دارد که فایل‌های مهمتان را برای همیشه از دست بدهید.

اما امروزه کار بک آپ گرفتن چندان سخت و گیج کننده نیست. شاید شما هم درباره انواع و اقسام روش‌های پشتیبان‌گیری شنیده باشید اما کدام گزینه برای شما مناسب‌تر است و واقعاً چه فایل‌هایی به بک آپ گرفتن نیاز دارند؟

٤-٢- مهم‌ترین مورد، اطلاعات شخصی است

اجازه بدهید اول از همه بحث را با بررسی این سؤال شروع کنیم که چه داده‌هایی واقعاً نیاز به پشتیبان‌گیری دارند؟ اولین و مهم‌ترین کار، بک آپ گرفتن از فایل‌های شخصی است چون در صورت ایجاد مشکل برای هارددیسک همیشه می‌توان سیستم‌عامل را دوباره نصب کرد و نرم‌افزارها را مجدداً دانلود کرد، اما اطلاعات شخصی غیر قابل جایگزینی هستند.

لازم است که به صورت منظم از داکیومنت‌ها، عکس‌ها، ویدیوهای خانگی و سایر اطلاعات موجود در کامپیوترتان پشتیبان‌گیری کنید. این موارد قابل جایگزینی نیستند. اگر ساعت‌های زیادی را صرف تبدیل سی‌دی‌های صوتی یا دی‌وی‌دی‌های تصویری کرده‌اید لازم است از این فایل‌ها هم پشتیبان‌گیری کنید تا نیازی نباشد که تمام این کارهای پرزحمت را دوباره انجام بدهید.

می‌توانید از سیستم‌عامل، نرم‌افزارها و سایر تنظیمات هم پشتیبان‌گیری کنید. ضرورتی برای انجام این کار نیست اما انجام این کار باعث می‌شود که در صورت ایجاد نقصی در هارددیسک کامپیوترتان، کار بازیابی آسان‌تر شود. اگر شما هم از جمله افرادی هستید که علاقه دارند دائم فایل‌های سیستم را دستکاری کنند، رجیستری را ویرایش کنند و یا مرتب سخت‌افزار را به‌روزرسانی کنند، داشتن بکاپی کامل از سیستم به شما کمک می‌کند تا در صورت ایجاد مشکل به میزان زیادی در زمان صرفه‌جویی کنید.

٤-٣- راه‌های بک آپ گرفتن از فایل‌ها

راه‌های بسیار زیادی برای پشتیبان گرفتن از داده‌ها وجود دارد، از استفاده از یک درایو اکسترنال گرفته تا پشتیبان‌گیری روی یک سرور ریموت از طریق اینترنت. در ادامه نقاط قوت و ضعف هر یک از این روش‌ها را بررسی می‌کنیم:

٤-٣-١- بک آپ گرفتن روی درایو اکسترنال

در صورتیکه هارد اکسترنال دارید، می‌توانید با استفاده از امکانات داخلی سیستم‌عامل، روی آن درایو پشتیبان‌گیری کنید. هر از گاهی درایو را به کامپیوتر وصل کرده و از ابزار پشتیبان‌گیری استفاده کنید یا اینکه هر زمان در منزل هستید آن را به کامپیوتر وصل کنید تا پشتیبان‌گیری به صورت خودکار انجام شود.

۱-۱-۳-۴- مزایا

پشتیبان‌گیری ارزان و سریع.

۲-۱-۳-۴- معایب

در صورتیکه کامپیوترتان دزدیده شود یا در حادثه‌ای مثل آتش‌سوزی از بین برود، فایل‌های پشتیبان شما هم با کامپیوترتان از بین خواهند رفت.

٤-٣-٢- بک آپ گرفتن از طریق اینترنت

اگر می‌خواهید مطمئن باشید که فایل‌های شما همیشه ایمن باقی می‌مانند، می‌توانید با استفاده از سرویسی مثلBackblaze از آن‌ها پشتیبان‌گیری کنید. بنابراین، در صورت از دست دادن فایل‌ها به هر دلیلی، می‌توانید آن‌ها را بازیابی کنید.

۱-۲-۳-۴- مزایا

پشتیبان‌گیری آنلاین می‌تواند با انواع روش‌های از بین رفتن داده از جمله نقص سخت‌افزاری دیسک، سرقت، بلایای طبیعی و هر مشکل دیگری مقابله کند.

۲-۲-۳-۴- معایب

معمولاً برای استفاده از این سرویس‌ها باید مبلغی را به صورت ماهیانه پرداخت کنید و معمولاً پشتیان گرفتن برای بار اول نسبت به پشتیبان‌گیری روی هارد زمان بیشتری می‌برد؛ بخصوص اگر تعداد فایل‌ها زیاد باشد.

٤-٣-٣- استفاده از یک سرویس ذخیره اطلاعات بر پایه فناوری ابر

شاید بعضی از متخصصین بر این باور باشند که این روش از لحاظ فنی روش پشتیبان‌گیری محسوب نمی‌شود اما واقعیت این است که این سیستم برای اکثر مردم قابلیت‌های موردنظرشان برای پشتیبان گیری از داده‌ها را دارد. به این ترتیب در صورتیکه مشکلی برای هارد کامپیوترتان ایجاد شود، یک یا چند نسخه از آن‌ها را خواهید داشت که به صورت آنلاین ذخیره شده‌اند.

۱-۳-۳-۴- مزایا

این روش سریع، آسان و در خیلی از موارد رایگان است و با توجه به آنلاین بودنش از بیشتر راه‌های از بین رفتن داده پیشگیری می‌کند.

۲-۳-۳-۴- معایب

خیلی از سرویس‌های ابری برای ذخیره اطلاعات محدودیت دارند بنابراین این روش تنها در صورتی کار می‌کند که تعداد فایل‌هایی که قرار است از آن‌ها پشتیبان‌گیری کنید، کم باشد یا این که برای رفع محدودیت، هزینه لازم را پرداخت کنید. بسته به فایل‌هایی که می‌خواهید از آن‌ها پشتیبان‌گیری کنید این روش ممکن است نسبت به نرم‌افزارهای پشتیبان‌گیری مستقیم، ساده‌تر یا پیچیده‌تر باشد.

٤-٤- یک بک آپ کافی نیست: از چند روش مختلف استفاده کنید

اما باید کدام‌یک از این روش‌ها را استفاده کرد؟ در حالت ایده آل باید حداقل از دو روش پشتیبان‌گیری استفاده کنید. چون بهتر است از اطلاعاتتان هم به صورت محلی یا Onsite و هم خارج از محل یا Offsite بک آپ داشته باشید.

حالتOnsite یعنی فایل‌های شما در حقیقت در همان محل فیزیکی‌ای ذخیره می‌شوند که خودتان در آن هستید؛ بنابراین اگر از فایل‌ها روی یک هارد اکسترنال پشتیبان‌گیری کنید و این هارد را در منزل و به همراه کامپیوترتان نگه دارید، این نسخه Onsite یا در محل محسوب می‌شود.

اما حالتOffsite یعنی فایل‌های شما در یک محل متفاوت نگه‌داری می‌شوند؛ بنابراین اگر از یک سرور آنلاین مثل Backblaze یا Dropbox استفاده کنید، در واقع از روش Offsite یا خارج از محل استفاده کرده‌اید.

پشتیبان‌گیری به روش Onsite سریع‌تر و آسان‌تر است و باید اولین خط دفاعی شما برای مقابله با از دست رفتن داده‌ها باشد. اگر به هر طریقی داده‌هایتان را از دست بدهید با این روش می‌توانید به سرعت آن‌ها را از روی هارد اکسترنال بازیابی کنید؛ اما نباید صرفاً به این روش متکی باشید چون اگر روزی منزل

شما دچار آتش‌سوزی شود یا سارقی تمام سخت‌افزارهای شما را به سرقت ببرد، در این صورت همه فایل‌هایتان را از دست خواهید داد.

نیازی نیست که روش‌های Offsite حتماً از طریق یک سرور در اینترنت انجام شوند و نیازی نیست که حتماً هزینه ماهیانه‌ای برای چنین سرویس‌هایی پرداخت کنید. می‌توانید از فایل‌هایتان روی یک هارد دیسک پشتیبان گرفته و بعد آن را مثلاً در اداره، منزل دوستتان یا در خزانه بانک نگه‌داری کنید. هر چند این روش دشواری‌هایی دارد اما این روش هم در اصل Offsite محسوب می‌شود.

٤-٥- بک آپ گرفتن را روی حالت اتوماتیک قرار دهید

هر چند ممکن است این موضوع پیچیده به نظر برسد اما هر چه سیستم پشتیبان‌گیری مورداستفاده‌تان را اتومات‌تر کنید، می‌توانید با فواصل زمانی کمتری از داده‌ها پشتیبان بگیرید و احتمال پشتیبان‌گیری منظم هم بیشتر خواهد شد. به همین دلیل توصیه می‌کنیم که به جای کپی کردن اطلاعات به صورت دستی روی درایو اکسترنال از یک ابزار اتوماتیک استفاده کنید. فقط کافیست این ابزار را یک بار تنظیم کنید.

نکته نهایی این که باید به محل نگهداری فایل‌ها خوب فکر کرده و اطمینان حاصل کنید که همیشه چندین نسخه از آن‌ها دارید. در حالت ایده آل این نسخه‌ها باید در بیش از یک موقعیت فیزیکی قرار داشته باشند. به این فکر کنید که اگر کامپیوترتان دچار مشکل شد باید چه طور با مشکل مقابله کنید، پس با پشتیبان گرفتن از اطلاعاتتان همیشه یک گام جلوتر از دیگران باشید.

فصل ۵– راهکارهای افزایش امنیت در فضای مجازی

در عصر فناورانه امروزی، انسان‌ها بخش عمده‌ای از وقت خود را در فضای مجازی گذرانده و صرف انجام کارهایی مثل بازدید و خرید از فروشگاه‌های اینترنتی، شبکه‌های اجتماعی، پیام‌رسان‌های ارتباطی، وبگردی و غیره می‌کنند. هکرها نیز از این فرصت سوءاستفاده کرده و تلاش می‌کنند با بهره‌گیری از روش‌های نوین حمله و ابزارهای مختلف؛ کاربران، سازمان‌ها و کسب‌وکارهای کوچک و بزرگ را مورد هدف قرار دهند.

مجرمان سایبری معمولاً از طریق ایمیل‌های حاوی فایل‌های پیوست آلوده یا لینک‌های مخرب، وب‌سایت‌های فروشگاهی جعلی و شبکه‌های اجتماعی، کاربران را فریب داده و با ارسال بدافزار یا نرم‌افزارهایی که امکان نفوذ، سرقت اطلاعات و جاسوسی از افراد را برای آنها فراهم می‌کنند، مخاطراتی را برای اشخاص و سازمان‌ها رقم می‌زنند.

۵-۱- افزایش امنیت در فضای مجازی با انجام اصول امنیت سایبری

با انجام موارد زیر می‌توانید از داده‌ها و اطلاعات‌تان در برابر نفوذگران اینترنتی محافظت کنید:

- استفاده از یک کلمه عبور قوی و مجزا برای هر یک از حساب‌های کاربری خود
- انتخاب کلمات عبور قوی و پیچیده، با ترکیب حداقل سه کلمه تصادفی
- ذخیره نکردن کلمه عبور در مرورگر
- فعال کردن احراز هویت دومرحله‌ای
- به‌روزرسانی مداوم دستگاه‌ها
- پشتیبان‌گیری مستمر از اطلاعات

۵-۱-۱- استفاده از یک کلمه عبور قوی و منحصربه‌فرد

هکرها می‌توانند با استفاده از نرم‌افزارهای مخصوص، کلمه عبور حساب‌های کاربری شما را کرک نموده و آنها را دوباره بازیابی کنند. آن‌ها برای انجام این کار، یک کلمه عبور را در وب‌سایت‌های مختلف امتحان کرده یا سعی می‌کنند از طریق روش‌های مختلف شما را تشویق به افشای گذرواژه‌تان کنند. هکرها در صورت دسترسی به ایمیل شما می‌توانند علاوه بر تغییر کلمه عبور آن به اطلاعات حساس و شخصی که درباره خودتان یا کسب‌وکارتان ذخیره کرده‌اید، به راحتی دسترسی پیدا کنند.

از این رو برای افزایش امنیت در فضای مجازی سعی کنید برای هر حساب کاربری از یک رمز متفاوت استفاده کرده و آن را به خاطر بسپارید. با انجام چنین کاری دیگر حدس یا کرک کردن کلمات عبور شما برای هکرها کار بسیار سختی خواهد بود.

۵-۱-۲- استفاده از کلمات عبور قوی و پیچیده

هنگامی که برای حساب‌های کاربری مهم خود از کلمات عبور متفاوت استفاده می‌کنید، شاید در وهله اول به خاطر سپردن همه آنها کار سختی باشد. یک روش کاربردی برای ایجاد کلمات عبور قوی که به راحتی نیز در ذهن سپرده شود، استفاده از ترکیبات متفاوت حداقل سه کلمه تصادفی است. توصیه می‌شود هرگز از کلماتی مثل نام حیوان خانگی‌تان یا کد ملی که به راحتی قابل حدس زدن است، استفاده نکنید. همچنین بهتر است از اعداد و نشانه‌ها هم در انتخاب کلمه عبورتان استفاده کنید.

۵-۱-۳- ذخیره نکردن کلمات عبور در مرورگر

اگرچه با ذخیره کلمات عبور در مرورگرها دیگر نیازی به خاطرسپاری آن‌ها نیست اما این اقدام علاوه بر اینکه شما را در برابر حملات سایبری آسیب‌پذیر می‌کند موجب افشای اطلاعات‌تان نیز می‌شود. کارشناسان امنیتی همواره به کاربران توصیه می‌کنند که از ذخیره کلمات عبورشان در مرورگرهای مختلف به شدت خودداری نمایند.

۵-۱-٤- فعال کردن احراز هویت دومرحله‌ای

فعال کردن احراز هویت دومرحله‌ای باعث می‌شود هکرها حتی در صورت داشتن کلمه عبور شما همچنان امکان دسترسی به حساب کاربری‌تان را نداشته باشند. عموماً برای بعضی از حساب‌های بانکی آنلاین، سرویس احراز هویت دومرحله‌ای به صورت خودکار فعال است. با انجام این کار برای اثبات هویت خودتان، اطلاعات شخصی بیشتری از شما درخواست شده و کد منحصربه‌فردی نیز به تلفن همراه شما ارسال می‌شود.

۵-۱-۵- به‌روزرسانی مداوم دستگاه‌ها

سیستم‌عامل‌ها، برنامه‌های کاربردی و نرم‌افزارهای منسوخ شده یا قدیمی معمولاً آسیب‌پذیری‌هایی دارند که به راحتی می‌توانند توسط نفوذگران مورد سوءاستفاده قرار گیرند. به همین خاطر همواره به انجام سریع به‌روزرسانی‌های برنامه‌ها و سیستم‌عامل توجه لازم را داشته باشید. با نصب این به‌روزرسانی‌ها مانع از نفوذ هکرها به سیستم‌ها و دسترسی به اطلاعات‌تان خواهید شد.

قابلیت به‌روزرسانی خودکار را برای نرم‌افزارها و دستگاه‌هایی که امکان پشتیبانی از این ویژگی را دارند، فعال کنید. البته بعضی از دستگاه‌ها و نرم‌افزارها هم باید به صورت دستی به‌روزرسانی شوند. برای انجام این کار می‌توانید هشدارهایی را جهت یادآوری، بر روی رایانه یا گوشی تلفن همراه‌تان تنظیم کنید. توجه داشته باشید که نصب به موقع به‌روزرسانی‌ها به حفظ امنیت‌تان در فضای آنلاین کمک زیادی می‌کند.

۵-۱-۶- پشتیبان‌گیری مستمر از اطلاعات

ممکن است در اثر وقوع یک حمله سایبری اطلاعات مهمی مثل عکس‌ها، اسناد، اطلاعات مالی یا اطلاعات مشتریان‌تان را از دست بدهید. با پشتیبان‌گیری منظم از اطلاعات‌تان می‌توانید شرایط را به سرعت بازیابی کرده و به حالت قبل از حمله برگردانید. برای انجام این کار باید یک نسخه از اطلاعات‌تان را بر روی یک دستگاه دیگر یا سرویس‌های ابری به صورت امن ذخیره کنید.

همچنین می‌توانید قابلیت پشتیبان‌گیری خودکار را فعال کرده تا اطلاعات شما به صورت منظم و خودکار بر روی بستر ابری ذخیره شوند. اگر از اطلاعات‌تان بر روی یک هارد اکسترنال یا حافظه USB پشتیبان‌گیری می‌کنید، هنگامی که قصد پشتیبان‌گیری از اطلاعات خود را ندارید حتماً این درایوها را از سیستم‌تان جدا کنید.

فصل ۶– حفاظت از زنجیره‌های تأمین در برابر حملات سایبری

کلیه سازمان‌ها، افراد، اطلاعات و منابعی که در همکاری با یکدیگر جهت عرضه یک محصول یا ارائه خدمت به مصرف‌کننده هستند یک سیستم زنجیره تأمین را تشکیل می‌دهند. هکرها با یک حمله هدفمند و ساده می‌توانند این سیستم را آلوده نموده و به تمام اعضای آن نفوذ کنند. بنابراین کلیه سازمان‌ها، کسب‌وکارها و صنایع باید آمادگی مقابله با حملات زنجیره تأمین را داشته باشند. در این مطلب از فراست یکسری از علل شیوع چشمگیر این حملات، دلایل ایجاد اختلالات عظیم در عملکرد سازمان‌ها توسط آنها و حفاظت از زنجیره‌های تأمین را مورد بررسی قرار می‌دهیم.

۶-۱- اعتماد

حملات زنجیره تأمین مشابه ایجاد آلودگی در منبع اصلی آب آشامیدنی به جای آلوده نمودن آب آشامیدنی گروه خاصی از موجودات زنده هستند. این حملات سیستم‌های سازمان‌های بسیار زیادی را آلوده نموده و قربانیان بیشتری را در بر می‌گیرند.

حملات زنجیره تأمین توسط هکرهایی انجام می‌شوند که از طریق دستکاری فرایندهای تولید یک قطعه فیزیکی یا در مسیر توزیع یک قطعه نرم‌افزاری، به سیستمی نفوذ نموده و بدافزارهای مدنظرشان را در برنامه‌های سالم اجرا می‌کنند. به این ترتیب امکان اجرای کدهای مخرب که شامل دسترسی‌هایی مشابه برنامه اصلی هستند برای آنها فراهم می‌شود.

برنامه‌های کاربردی مجاز و مورد اطمینان قابلیت ایجاد پوششی را برای کدهای مخرب و بدافزارها دارند. به این ترتیب این آلودگی‌ها با همان دسترسی‌ها و سطح اعتماد برنامه اصلی، در سرتاسر زنجیره تأمین توزیع می‌گردند. هکرها با سوءاستفاده از چنین قابلیت اطمینان و اعتمادی می‌توانند بدون اینکه شناسایی شوند، یک نفوذ گسترده انجام دهند.

اجرای بدافزارها در برنامه‌ها و سیستم‌های سالم در هر مرحله‌ای از چرخه حیات محصول قابل انجام بوده و فرصت‌های خاصی را برای نفوذ فراهم می‌کند. همچنین وجود حتی یک حلقه ضعیف هم می‌تواند مخاطرات امنیتی بسیار زیادی را برای کل زنجیره تأمین ایجاد نماید. هک زنجیره تأمین معمولاً در مراحل اولیه چرخه تولید نرم‌افزار رخ می‌دهد. از این رو هرچقدر هم که سیستم امنیتی کاربران نهایی قوی باشد، آن‌ها همچنان در برابر حملات زنجیره تأمین آسیب‌پذیر هستند. از طرفی دیگر گسترش و پیچیدگی بسیاری از عملیات سازمان‌ها منجر به افزایش مراحل زنجیره تأمین شده است. درنتیجه هکرها فرصت‌های بیشتری برای نفوذ در اختیار دارند. همچنین با توجه به عدم تسلط سازمان‌ها به نقشه کل مراحل اجرای زنجیره تأمین شانس شناسایی مجرمان سایبری بسیار پایین است.

۶-۲- حمله به مرکز جهت ایجاد خرابکاری وسیع

افزایش کاربرد فناوری در بخش‌ها و گرایش‌های مختلف و توسعه زیرساخت اینترنت اشیا در حوزه‌هایی مثل درمان، صنایع نظامی و مالی، امکان دسترسی وسیع هکرها به اطلاعات حساس را فراهم نموده است. با توجه به فعالیت این صنایع و کسب‌وکارها در مقیاس عظیم و همچنین گسترش سیستم‌های زنجیره تأمین، چنین دسترسی‌هایی فرصت‌های بسیار زیادی را برای حمله ایجاد کرده و پیامدهای مخرب بی‌شماری را به بار می‌آورند.

در سال ۲۰۲۱ میلادی محققان اعلام کردند که مهاجمان از سال ۲۰۱۲ تا کنون از یک رابط کاربری یکپارچه توسعه‌پذیر میان‌افزار برای ایجاد در پشتی در سیستم‌های ویندوزی استفاده می‌کنند. این بدافزار قابلیت دور زدن سازوکارهای امنیتی ویندوز برای بارگذاری درایور بدون امضای خودش، سرقت اسناد، ثبت ضربات وارد شده به صفحه کلید و ایجاد اسکرین‌شات‌های منظم از صفحه نمایش کاربر را دارد. مهاجمان پس از نفوذ به مراحل ابتدایی فرایند بوت شدن سیستم امکان دور زدن راهکارهای امنیتی را برای بدافزارها فراهم نموده و درایور مخرب‌شان را در هنگام روشن شدن سیستم بارگذاری کردند. واضح است که با وجود پیاده‌سازی همه سازوکارهای امنیتی پیشرفته در سمت کاربر نهایی، حتی وجود یک نقطه ضعف امنیتی در زنجیره تولید یک محصول هم می‌تواند امنیت کل سیستم را دچار مخاطره کند.

شرکت‌های مختلف در آمریکای شمالی و اروپا نیز مورد هدف نمونه‌ای دیگر از حملات زنجیره تأمین پیچیده قرار گرفتند. این حمله توسط گروه جاسوسی سایبری Dragonfly اجرا شد. این گروه ابتدا به نرم‌افزارهای کنترل صنعتی نفوذ کرده و فایل‌های مخرب و آلوده را جایگزین فایل‌های سالم می‌کردند. به این ترتیب هکرهای این گروه پس از تبدیل فایل‌های اصلی به تروجان‌هایی برای بدافزار خودشان و بدون این که شناسایی شوند در مسیر زنجیره تأمین حرکت کردند.

هکرها می‌توانند ضعیف‌ترین حلقه در زنجیره تأمین را تشخیص داده و دستگاه‌ها را پیش از توزیع آلوده و دستکاری کنند؛ بنابراین امکان نفوذ به تجهیزات اینترنت اشیا و سخت‌افزارها نیز به راحتی وجود دارد. همچنین ممکن است بدافزاری که سازوکارهای زنجیره تأمین را دور زده و از آن گذشته امکان دسترسی از راه دور و کنترل سیستم‌ها را برای هکرها فراهم کند. حجم انبوه اطلاعات شخصی، هویتی و مالی که در دستگاه‌های مختلف ذخیره می‌شود منجر به افزایش جذابیت این منابع برای هکرها و مخاطرات امنیتی برعلیه سیستم‌های زنجیره تأمین شده است.

٦-٣- شناسایی در نقطه حمله

تشخیص اینکه آیا واقعاً یک دستگاه یا سیستم دستکاری شده و همچنین مشخص نمودن وضعیت امنیتی نقاط پایانی مختلف در شبکه کار چندان ساده‌ای نیست. به‌تازگی Trusted Computing مجموعه‌ای از ویژگی‌ها و یک راهنمای رسمی جهت ارزیابی جامعیت میان‌افزارها و سنجش عملکرد تجهیزات خریداری شده توسط سازمان‌ها را منتشر نموده است. این راهنما یک چارچوب مشخص برای تعیین مبنای جامعیت میان‌افزارهای در حال اجرا بر روی یک دستگاه را فراهم می‌کند. به این ترتیب امکان شناسایی مخاطرات موجود در چرخه حیات یک محصول وجود دارد. انتشار این مجموعه برای زنجیره‌های تولید وسیعی که شامل مسیر زنجیره تأمین بسیار پیچیده هستند، یک پیشرفت مهم و اساسی محسوب می‌شود.

مهاجمانی که زنجیره‌های تأمین را مورد هدف قرار می‌دهند معمولاً فرض می‌کنند که بدافزار آنها در کل این زنجیره قابل شناسایی نیست. در حالی که تولیدکننده یا کاربر نهایی می‌تواند با استفاده از راهنمایی‌ها و هشدارهای جامع موجود عملکرد نهایی دستگاه و شبکه‌ها را بررسی کند. به این ترتیب امکان تشخیص همه تهدیدات در کلیه مراحل یک زنجیره تأمین وجود دارد. همچنین شناسایی هر نقطه دسترسی ضعیف و اصلاح آن، تعداد دستگاه‌های در معرض خطر و احتمال وقوع حملات آتی را کاهش می‌دهد.

٦-٤- حفاظت از زنجیره‌های تأمین

در صورت شناسایی زودهنگام تهدیداتی که در مسیر زنجیره تأمین قرار دارند، احتمال ایجاد آسیب برای سایر بخش‌های زنجیره تأمین کمتر می‌شود. از طرفی دیگر نرم‌افزارها و سخت‌افزارهای آلوده از مسیر زنجیره تأمین عبور نکرده و وارد سیستم کاربران نهایی نمی‌شوند. بررسی جامعیت و سنجش و ارزیابی عملکرد سخت‌افزار و نرم‌افزار در هر نقطه از زنجیره تأمین، امکان شناسایی و رفع نقطه ضعف‌ها پیش از وقوع رخنه امنیتی را فراهم نموده و احتمال عدم تشخیص نفوذ هکرها را کاهش می‌دهد.

فصل ۷– مقابله با چالش‌های در حال تحول سایبری در خدمات مالی

فناوری‌های دیجیتال از جمله فناوری‌های اتوماسیون مثل هوش مصنوعی و یادگیری ماشینی که کارایی عملیات بانکی را افزایش داده و تجربیات کاربری مطلوب‌تری ایجاد می‌کنند مانند سایر بخش‌های اقتصاد، در حوزه خدمات مالی نقش مهمی دارند.

با حرکت گسترده افراد و کسب‌وکارها به سمت تراکنش‌های مالی و بانکداری دیجیتال به‌ویژه پس از شیوع ویروس کرونا، مجرمان سایبری نیز همواره در حال تلاش برای حمله و نفوذ به این بخش‌ها با استفاده از روش‌های حرفه‌ای بودند؛ بنابراین بخش زیادی از حملات سایبری در سال‌های اخیر ناشی از جرائم مالی است.

۷-۱- میزان هم‌پوشانی جرائم مالی و جرائم سایبری

با توجه به وجود عنصر فناوری در حملات سایبری که امکان سوءاستفاده از آسیب‌پذیری‌های فنی را فراهم می‌کند، این جرائم بیشترین رقم حملات سایبری مالی را به خود اختصاص داده‌اند اما به تازگی رویکردی که در این زمینه وجود دارد تغییر کرده است.

البته پیش از این شرایط بسیار ساده‌تر بود. در گذشته یک کلاهبردار پس از هک یک کامپیوتر یا لپ‌تاپ، ابزاری را جهت پیگیری فعالیت در مرورگر نصب می‌کرد. سپس زمانی که کاربر وارد حساب بانکی خودش می‌شد، مهاجمان هم به این حساب دسترسی پیدا نموده و از آن برای پولشویی یا سرقت استفاده می‌کردند. این مثال نشان‌دهنده همپوشانی جرائم مالی و جرائم سایبری در سطحی ساده است.

در حال حاضر شرایط بسیار پیچیده بوده و چالش اصلی مربوط به نفوذ به فرایندها در مقیاس عظیم است. مجرمان به جای حمله به سیستم‌های امنیتی به سیستم‌های هوش مصنوعی و اتوماسیون حمله می‌کنند. سازمان‌ها برای انجام کارهای آنلاین خود به آنها وابسته هستند. امروزه مجرمان در قالب نقش‌های تخصصی گروه‌بندی شده و می‌توانند مستندات و هویت‌های جعلی جدیدی ایجاد کنند و آنها را وارد سیستم اقتصادی نمایند. به این ترتیب مجرمان می‌توانند در هر ساعت هزاران تنظیم مختلف را تغییر داده و در نهایت اطلاعات جمع‌آوری شده را برای ارتکاب جرم به دیگران می‌فروشند. در این روش همه تراکنش‌ها در فضای آنلاین اجرا شده و در نتیجه نیاز به ملاقات رودررو وجود ندارد.

این فرایند نفوذ و هک مرز بین جعل، پولشویی و جرائم سایبری را کمرنگ‌تر کرده است؛ بنابراین تیم‌هایی که پیش از این مسئول رسیدگی به مخاطرات کلاهبرداری و رعایت استانداردها و قوانین بوده‌اند، باید مشابه کارشناسان امنیت سایبری فکر کنند. آن‌ها باید در این مسیر داده‌ها و اطلاعات موجود درباره

چشم‌انداز تهدیدات، افراد، فناوری‌ها و فرایندها را جمع‌آوری نموده و دشمن را در مسیر دستیابی به اهدافش ناکام بگذارند.

پیچیدگی در شناسایی و مقابله با این حملات معمولاً ناشی از روش پیاده‌سازی آنها است. روش‌های سنتی متکی بر روی نیروی کار انسانی و مداخله آنها سرعت لازم برای به چالش کشیدن جعل هویت را نداشته و بسیار زمانبر هستند. براساس شواهد امروزی اعتماد به اتوماسیون ساده یا هوش مصنوعی مبتنی بر قاعده برای رسیدگی به این حملات کافی نیست. حتی سیستم‌های هوش مصنوعی هوشمندتری که نگاهی به مشتریان ورودی ندارند هم نمی‌توانند با این موج از حملات مقابله کنند.

بنابراین به یک روش شناسایی جرائم هویتی به صورت بلادرنگ نیاز داریم. چنین روشی در تأیید هویت افراد و اینکه هویت یک مشتری به خطر افتاده و بیش از این قابل اعتماد نیست نقش مؤثری دارد.

شیوع بیماری کرونا به شناسایی آسیب‌پذیری‌های موجود در پلتفرم‌های دیجیتال امروزی که قابلیت اجرای تراکنش به صورت فوری را دارند، کمک کرد. در چنین سیستم‌هایی فرصت محدودی برای اعتبارسنجی تراکنش یا تأیید هویت مشتری وجود دارد. به همین ترتیب پیچیدگی‌های فرایند احراز هویت مشتریان و افزودن مشتریان جدید در عصر دیجیتال، سازمان‌های حوزه خدمات مالی و مشتریان آنها را در معرض مخاطرات روزافزون جرائم سایبری و کلاهبرداری قرار می‌دهد.

توسعه سریع اتوماسیون در حوزه خدمات مالی برای ساده‌سازی کار مشتریان منجر به ایجاد چالش‌های جدیدی در حوزه سیاست‌ها و شیوه‌های مدیریت ریسک و اعتبارسنجی شده است. در حال حاضر ارزیابی اصالت یک تعامل دیجیتال مستلزم بررسی انبوهی از داده‌ها از جنبه‌های مختلف از جمله موقعیت مکانی، رفتارهای کاربر در هر نشست، داده‌های به دست آمده از فروشندگان و غیره است.

علاوه بر این، مهاجمان امروزی همواره در زمینه هدف گرفتن این محیط‌های دیجیتال پیچیده توانایی بیشتری پیدا نموده و از فناوری‌های نوینی مثل بلاک‌چین و پرداخت فوری بر ضد بانک‌ها و مشتریان آنها استفاده می‌کنند.

۷-۲- سازمان‌ها چگونه باید با این تهدیدات مقابله کنند؟

راهکارهای هوش مصنوعی و یادگیری ماشینی تنها روش‌های مقیاس‌پذیری هستند که می‌توانند به صورت بلادرنگ بر روی سیستم‌های اقتصادی نظارت کنند. همچنین لازم است به مدارک جدید و ارزیابی رفتار مشتریان نظارت داشت تا هویت‌های جعلی، تلاش برای تصاحب حساب‌های کاربری، پولشویی و سایر انواع کلاهبرداری که ریشه سایبری دارند شناسایی شوند. استفاده از سیستمی متشکل از الگوریتم‌ها، روش‌ها

و داده‌هایی که همواره در حال تغییر و بهبود هستند برای تشخیص الگوهای حملات هم به مقابله با تهدیدات کمک می‌کند.

در عین حال لازم به ذکر است که مهاجمان سایبری نیز از یادگیری ماشینی و هوش مصنوعی برای اجرای فعالیت‌های خودشان استفاده می‌کنند؛ بنابراین این شرایط مشابه یک بازی موش و گربه است که حوزه خدمات مالی باید برای پیروزی در آن همواره در حال رشد و تکامل باشد.

ابزارهای جرم‌شناسایی بلادرنگ مجهز به هوش مصنوعی می‌توانند جرائم اقتصادی پیشرفته، جعل و دستکاری را شناسایی کنند و قابلیت شناسایی آسیب‌پذیری‌های موجود در سیستم‌ها برای پیشگیری از سوءاستفاده‌های آینده را دارند.

فصل ۸– آشنایی با سه اصطلاحCERT ، CSIRT وSOC

آشنایی با اصطلاحات مهم است چون استفاده نادرست از آنها باعث ایجاد سوءتفاهم در درک توضیحات و ایجاد ابهام برای تیم واکنش به حادثه می‌شود.

CSIRT،CERT، CIRTو SOC از جمله اصطلاحاتی هستند که در حوزه واکنش به حادثه زیاد به گوش می‌خورند. سه عبارت اول به عنوان مترادف هم و برای توصیف تیم‌هایی به کار می‌روند که متمرکز بر واکنش به حادثه هستند. SOC نیز کاربرد وسیع‌تری در حوزه امنیت و امنیت سایبری دارد.

۸-۱- CERT، CSIRTو CIRT مخفف چه کلماتی هستند؟

ابتدا اصطلاحاتی را که رایج‌ترین مدل‌های سازمانی تیم‌های واکنش به حادثه شرح می‌دهند را مورد بررسی قرار می‌دهیم. البته دقت کنید اینکه مثلاً دو سازمان به تیم واکنش خودشان CSIRT می‌گویند، به این معنا نیست که هر دو تیم اهداف یا روش‌های مشابهی دارند یا با یک تعریف ایده‌آل‌سازی شده همخوانی دارند.

CSIRT مخفف تیم واکنش به حوادث امنیتی کامپیوتری است.CERT مخفف تیم واکنش برای شرایط اضطراری کامپیوتری است. CIRT هم می‌تواند مخفف تیم واکنش به حوادث کامپیوتری یا تیم واکنش به حوادث امنیت سایبری باشد (که حالت اول رایج‌تر است). از CSIRT، CERTو CIRT معمولاً به جای یکدیگر استفاده می‌شود. در واقع، CSIRTو CIRT تقریباً معادل و مترادف هم هستند. ممکن است یک سازمان بر اساس سبک یا زبان خاص خودش یا تفاوت‌های جزئی در محدوده سازمانی، یکی از این موارد را ترجیح دهد.

۸-۲- CERTچیست؟

اگرچه سازمان‌ها معمولاً از این اصطلاح به صورت عمومی استفاده می‌کنند اما از سال ۱۹۹۷ نشان تجاری آن برای دانشگاه کارنگی ثبت شد. شرکت‌ها می‌توانند درخواست استفاده از نشان تجاری CERT را ثبت کنند. شرکت‌هایی که این درخواست را ثبت نکنند اجازه استفاده از این اصطلاح را در نام خدمات مشاوره یا به عنوان ارائه‌دهنده خدمات امنیتی مدیریت شده ندارند؛ بنابراین اگر سازمانی قصد استفاده از اصطلاح CERT به عنوان بخشی از نام تیم واکنش خودش را دارد، بهتر است که در این رابطه با یک مشاور حقوقی گفتگو کند.

یکی از چالش‌های استفاده از CERT به عنوان نام، احتمال گیج‌کننده بودن آن است. مثلاً ممکن است تصور شود که از CERT به عنوان مترادف CSIRT استفاده شده یا اینکه سازمان سعی در انتقال مفهومی متفاوت دارد. با توجه به شرایط، احتمال صحیح بودن هر دو حالت وجود دارد.

اصطلاح CERT مورد استفاده دانشگاه کارنگی ملون تمرکز و حوزه خاصی دارد و به عنوان یک همکار با نهادهای دولتی، صنعتی، مجریان قانون و دانشگاه عمل می‌کند تا امنیت و مقاومت شبکه‌ها و سیستم‌های کامپیوتری را تقویت کند. استفاده از این اصطلاح به معنای مطالعه درباره مسائلی با پیامدهای امنیتی گسترده و طراحی ابزارها و روش‌های پیشرفته است.

برخی سازمان‌ها این موضوع را در شیوه استفاده از این اصطلاح منعکس می‌کنند. به عبارتی این سازمان‌ها از CERT استفاده می‌کنند تا نشان دهند که تمرکز تیم داخلی‌شان نسبت به تمرکز یک CSIRT معمولی متفاوت است. مثلاً ممکن است تیمی که مایل به همکاری با سایر سازمان‌ها یا تیم‌های داخلی یا خارجی است، تمرکز اصلی خود را بر توسعه ابزار و روش‌های پیش‌بینی مشکلات و غیره یا مطالعه تهدیدات نوظهور از جمله اصول تجارت یا روش‌های دشمنان بگزارد؛ بنابراین کاربرد اصطلاح CERT معمولاً در حوزه ارتقای واکنش به حادثه به عنوان یک رشته است.

همچنین سازمان‌هایی که از CERT استفاده می‌کنند اما از وضعیت CERT به عنوان یک نشان تجاری ثبت شده آگاه نیستند، بیشتر این اصطلاح را به عنوان مترادف CIRT یا CSIRT در نظر می‌گیرند.

۸-۳- تفاوت بین CERT ، CSIRT و CIRT

ممکن است گروه‌های CERT، CSIRT و CIRT با استفاده از کارمندانی دائم تشکیل شوند یا اینکه بر حسب شرایط و در واکنش به یک رویداد شکل بگیرند. در هر صورت همواره تمرکز این گروه‌ها تقریباً چهار مرحله از واکنش به حادثه است که در راهنمای رسیدگی به حوادث امنیت کامپیوتری NIST معرفی شده‌اند:

- آمادگی؛
- تشخیص و تحلیل؛
- مهار، ریشه‌کنی و بازیابی؛
- فعالیت‌های پس از حادثه

این مراحل متمرکز بر تشخیص و مهار حوادث امنیتی هستند. همچینن شامل ساختارهای حاکمیتی هستند که یک سازمان با هدف آمادگی جهت مواجهه با حوادث امنیتی از آنها استفاده می‌کند و فعالیت‌های پس از حادثه‌ای که برای هموارسازی تلاش‌های آینده طراحی شده‌اند.

البته یکسری ظرافت در این زمینه وجود دارد. لزوماً هر گروهی در هر سازمانی کارهای مشابهی انجام نمی‌دهد. ممکن است نحوه استفاده برخی تیم‌ها از CSIRT با راهنمای NIST همخوانی داشته باشد اما تغییرات و اصلاحاتی در عملکردشان اعمال کنند. مثلاً یک سازمان نقش CSIRT را متمرکز بر سیاست و دیگری بر مسائل عملیاتی بداند مثل بررسی فایل‌های گزارش و پیگیری فعالیت‌ها در شبکه.

مرکز عملیات امنیتی (SOC[3]) یکی دیگر از اصطلاحات پرکاربرد در حوزه واکنش به حادثه است اما به طور کلی SOC شامل چندین جنبه از عملیات امنیتی است در حالی کهCSIRT ، CERTو CIRT به طور ویژه متمرکز بر واکنش به حادثه هستند. محدوده عملکرد SOC می‌تواند واکنش به حادثه (کامل یا جزئی) و همچنین فعالیت‌های دیگر را شامل شود. برای مثال، یک SOC می‌تواند:

- عملیات کنترل و نظارت را پوشش دهد (مثل سیستم تشخیص نفوذ، سیستم پیشگیری از تشخیص نفوذ، سیستم مدیریت اطلاعات امنیتی، سیستم مدیریت رویدادهای اطلاعات امنیتی)؛
- نظارت بر عملکرد امنیتی و عملیاتی و گردآوری اطلاعات؛
- مدیریت کارهایی مثل مجوزدهی و مدیریت هویت، نگهداری از مجموعه قوانین فیلترینگ و فایروال (هم نظارت و هم مدیریت تغییرات)، پشتیبانی از تحقیقات و جرم‌شناسی و سایر جنبه‌های امنیت عملیاتی.

CSIRTو CERT به طور ویژه متمرکز بر واکنش به حادثه هستند. از این دو اصطلاح معمولاً به عنوان مترادف استفاده می‌شود اما از لحاظ فنی متفاوت هستند. از جمله اینکه اصطلاح CERT به عنوان یک نشان تجاری ثبت شده اما CSIRT معمولاً با یک تیم تجاری دارای عملکرد متقابل سروکار دارد. محدوده عملکرد SOC هم بر خلاف دو مورد اول گسترده‌تر از واکنش به حادثه است و به سایر حوزه‌های امنیت هم گسترش پیدا می‌کند.

تلاش‌های نظارتی SOC فراتر از واکنش به حادثه هستند. ممکن است SOC شاخص‌های آماری لازم برای پشتیبانی از مشتریان یا ارائه خدمات را گردآوری کند یا احتمال دارد از گزارش‌های مدیریتی پشتیبانی کند مثل آماده‌سازی معیارها و داده‌ها برای حمایت از ارزیابی ریسک یا جهت پشتیبانی از حسابرسی‌ها. اگرچه معمولاً SOC در حوزه واکنش به حادثه فعالیت دارد اما تقریباً همیشه سایر حوزه‌های امنیت را هم پوشش می‌دهد. همچنین کاربرد و هدف عملیاتی SOC گسترده‌تر از CSIRT یا CIRT است. اگر در سازمانی

یک SOC وجود داشته باشد، احتمالاً واکنش به حادثه جزو مسئولیت‌های این بخش خواهد بود. همچنان جزئیات این مسئولیت‌ها و تعریف‌ها بستگی به سازمان مد نظر دارد.

۸-٤- CERT/CSIRT/CIRT یا SOC کدامیک را پیاده‌سازی کنیم؟

سازمان‌ها با داشتن درکی واضح از این اصطلاحات می‌توانند تشخیص دهند که چه مدلی از تیم واکنش به حادثه برای آنها مناسب است و چگونه می‌توانند این تیم را تشکیل دهند. این انتخاب باید با توجه به اهداف، ساختار و استفاده از منابع سازمان انجام شود. مثلاً اگر نیاز به نظارت الزامی است و ساختار سازمانی شما بنحوی است که امکان متمرکزسازی این فعالیت‌ها را در یک محل فیزیکی یا منطقی فراهم می‌کند، احتمالاً تشکیل SOC برای شما مناسب‌تر است (مثلاً با توجه به اقتصاد مقیاس یا سادگی سلسله مراتب گزارش‌دهی). در مقابل اگر ساختار سازمان شما غیرمتمرکزتر است یا متمرکزسازی نظارت و سایر عملیات امنیتی برای شما مناسب و سازنده نیست، ممکن است CSIRT بیشتر مناسب شما باشد.

فصل ۹– دیده شدن دارایی پایه و اساس امنیت سایبری

قابلیت نظارت بر روی دارایی‌ها، پایه و اساس اصلی طرح‌های کارآمد برای حفاظت از امنیت سایبری فناوری عملیاتی است. از طرفی سازمان‌های صنعتی نمی‌توانند ایمنی دارایی‌هایی را که چندان با آنها آشنا نیستند حفظ کنند. همه سازمان‌ها صرف‌نظر از نوع فعالیت‌شان باید قابلیت نظارت بر روی اطلاعات حساس و کنترل آنها را داشته باشند. حملات سایبری علاوه بر ایمنی، ممکن است زمان فعالیت و حتی دسترس‌پذیری همه ابزارها از توربین‌ها گرفته تا کنترل‌کننده‌های دما و غیره را تحت تأثیر قرار دهند. شناسایی و ثبت کامل تجهیزات فناوری عملیاتی توسط سازمان‌ها و تشکیل پایه‌های لازم منجر به ساده‌سازی فرایندهای امنیت سایبری مثل تشخیص تهدید، واکنش به حادثه، مدیریت فعالانه دارایی‌ها برای شناسایی آسیب‌پذیری‌ها و نقاط ضعف و پیاده‌سازی طرح‌های امنیتی استراتژیک در محیط‌های فناوری عملیاتی خواهند شد.

مدیران اجرایی که فهرست دقیقی از موجودی‌های خود و طبقه‌بندی‌های موجود ندارند، در صورت مواجه با تهدیدات فناوری عملیاتی تأثیرگذار بر روی سیستم‌های مختلف، چگونه می‌توانند ارتباط این تهدیدات نوظهور با کسب‌وکار خودشان را تشخیص دهند؟ فقط با نظارت پیوسته بر روی تجهیزات فناوری عملیاتی، امکان شناسایی مسائل و مشکلات زیر وجود دارد:

- کانال‌های ارتباطی که متصدیان از وجودشان اطلاعی ندارند؛
- تهدیدات فعالی که به صورت مخفیانه در محیط عمل می‌کنند؛
- پیکربندی‌های ناامن؛
- آسیب‌پذیری‌های مخفی؛
- تجهیزات مشکل‌آفرین و غیره.

میزان بهم پیوستگی و اتصالات دنیای ما رو به افزایش است؛ بنابراین شرکت‌ها می‌توانند جهت شناسایی دارایی‌ها و داده‌های خودشان از افراد مرتبط درباره اطلاعات و دارایی‌هایی که در اختیار دارند پرس‌وجو کنند. البته سازمان‌ها معمولاً پاسخ‌های متفاوتی از بخش‌های آی‌تی، امنیت یا عملیات دریافت می‌نمایند. از این رو همه افراد سازمان تصویر واضحی از دارایی‌های شبکه ندارند و این موضوع یک زنگ خطر است.

۹-۱- حذف خلأ دید

شرکت‌ها عموماً می‌دانند که باید فهرست دارایی‌های خودشان را ثبت کنند ولی اجرای یک روش کارآمد تأثیر زیادی بر روی بهره‌وری جمع‌آوری داده‌ها و رفع مشکلات امنیتی دارد. حجم داده‌های تولید شده

معمولاً با سرعت زیادی افزایش می‌یابد. از این رو درک الزامات حیاتی و اهداف مطلوب سازمان در زمینه مدیریت ریسک یا کسب‌وکار تأثیر چشمگیری در پیشگیری از بروز مشکلات مخاطره‌آمیز دارد.

فناوری اطلاعات دارای سابقه و میراثی طولانی در زمینه مدیریت و ثبت فهرست دارایی‌ها بوده و ابزارها، فریم‌ورک‌ها و شیوه‌های ایجاد قابلیت دید بر روی این دارایی‌ها متناسب با کاربردهایشان تنظیم و بهینه‌سازی شده‌اند. با این وجود اگرچه ابزارها و فرایندهای بخش فناوری اطلاعات متناسب با چالش‌های موجود در محیط فناوری عملیاتی طراحی نشده‌اند ولی در هر صورت این چالش‌ها باید جهت حفاظت از دارایی‌های صنعتی مدیریت گردند. کارمندان اداری معمولاً تجربه ریبوت اجباری کامپیوترها برای نصب وصله‌های امنیتی را دارند اما در یک محیط صنعتی، راه‌اندازی مجدد یک ایستگاه کاری متصل به یک کوره ذوب یا همان ریبوت می‌تواند منجر به از کارافتادگی برنامه‌ریزی نشده در تجهیزات خنک‌کننده، تخلیه‌کننده و گرم‌کننده کوره در طی مدت زمانی طولانی شود.

بسیاری از تاکتیک‌ها و ابزارهایی که جهت نظارت بر روی دارایی‌های فناوری اطلاعات طراحی شده‌اند، معمولاً قابل تبدیل برای استفاده در محیط فناوری عملیاتی نیستند. برای مثال امکان استقرار یک کارگذار بر روی یک PLC وجود ندارد چون این تجهیزات معمولاً با سیستم‌عامل‌ها یا میان‌افزارهایی کار می‌کنند که سازگاری چندانی با کارگذارها ندارند. یک مدیر فناوری اطلاعات که با استفاده از ابزارNMAP ، اسکن شبکه را در یک محیط صنعتی اجرا می‌کند، ممکن است ناخواسته باعث غیرفعال‌سازی دستگاه‌های حساس مثل کنترل‌گرهای دستگاه شود. در نتیجه در چنین شرایطی امکان بروز اختلال در خط تولید یا توقف آن وجود دارد. در محیط‌های فناوری اطلاعات سنتی، استفاده از ابزارهای اسکن فعال برای شناسایی و نظارت بر روی دارایی‌ها یک امر کاملاً عادی است. در هر صورت اجرای تکنیک‌های غیرفعال که ایمنی بیشتری ایجاد می‌کنند ترجیح داده می‌شوند. سازمان‌ها باید برای تحقق نظارت مناسب بر روی دارایی‌های محیط فناوری عملیاتی، یک رویکرد متفاوت و مناسب با این محیط بکار بگیرند.

یکی از راهنماهای توصیه شده به مالکان دارایی‌های فناوری عملیاتی، استفاده از فریم‌ورک مدیریت مجموعه برای واکنش به حادثه و عملیات امنیتی ICS است. این منبع شامل یک مرجع کامل است که طی سال‌ها تجربه شکل گرفته و با واقعیت‌های منحصربفرد محیط فناوری عملیاتی سازگاری دارد. در ادامه ابتدا دلایل نیاز به نظارت و سپس اصول و پایه‌های فریم‌ورک مدیریت مجموعه و نحوه دستیابی به نظارت بر روی دارایی‌ها را مورد بررسی قرار می‌دهیم.

براساس نظرسنجی که در سال ۲۰۱۹ توسط مؤسسه SANS صورت گرفته، فقط حدود ۱۰ درصد از سازمان‌ها فهرست کامل دارایی‌های تحت پوشش مرکز عملیات امنیتی را در اختیار دارند.

همچنین با توجه به مطالعه امنیت سایبری ICS شرکت Dragos که در سال ۲۰۲۰ میلادی انجام شده، در حدود ۹۰ درصد از تعاملات این شرکت با سایر شرکت‌ها برای ارائه خدمات حرفه‌ای، مشخص شده که سازمان‌ها دید نسبتاً محدودی بر روی محیط فناوری عملیاتی خودشان دارند یا اینکه دارای هیچ‌گونه قدرتی برای نظارت و کنترلی بر روی دارایی‌های خود نیستند.

وجود فهرست دارایی‌های مهم برای انجام یک عملیات نقش مهمی در مدیریت ریسک امنیت سایبری دارد. ثبت اطلاعات حساس مثل نسخه نرم‌افزار، موقعیت فیزیکی، مالک دستگاه و الویت آن به انجام سایر فعالیت‌ها و عملیات ضروری جهت مدیریت امنیت سایبری کمک می‌کند

۹-۲- راهکارهای نظارت بر روی دارایی‌ها

۹-۲-۱- مشخص نمودن وضعیت عادی

آشنایی با وضعیت واقعی محیط و اینکه چه دارایی‌هایی در کدام قسمت از شبکه قرار دارند و دارای چه عملکردی هستند، منجر به ایجاد یک خط مبنا و الگو از شرایط عادی می‌شود. برای مثال شما انتظار ندارید که یک سرور مدیریت وصله‌های امنیتی ناگهان شروع به ارسال موقعیت مکانی به یک منبع خاص در اینترنت کند. با پیاده‌سازی چنین الگویی می‌توانید نحوه اجرای فرایندها و جریانات کاری را در محیط عملیاتی مشخص نمایید. همچنین این منبع زمینه لازم و اطلاعات شفاف برای تسریع فعالیت‌های امنیتی مختلف مثل تشخیص تهدید، نظارت، مدیریت تغییر و واکنش به حادثه را فراهم می‌کند.

برقراری این خط مبنا فقط با هدف پیگیری حلقه تشخیص ناهنجاری انجام نمی‌شود. وابستگی صرف به تشخیص ناهنجاری می‌تواند باعث بروز مشکلات مختلف و خستگی از هشدارهای متعدد شود چون ناهنجاری همواره معادل با تهدید نیست. البته شناسایی وضعیت عادی و تشخیص هر گونه تخدی از این خط مبنا می‌تواند داده‌ها و تاریخچه‌های مفیدی در اختیار تحلیلگران امنیت قرار دهد. کارشناسان امنیتی نیز می‌توانند از چنین اطلاعاتی در بررسی‌ها و همچنین جهت انجام اقدامات لازم استفاده کنند.

متصدیان سیستم‌ها به ابزارهایی جهت ارتقای بهره‌وری، تشخیص راحت خط مبنا و شناسایی سریع هرگونه انحراف از این خط مبنا نیاز دارند. این تشخیص‌ها معمولاً در اثر هشدارها یا اعلان‌ها صورت می‌گیرند. البته می‌توانند قالب‌ها و نمودارهای گرافیکی هم داشته باشند. رنگ‌های مختلف در این نمودارها نشان‌دهنده وضعیت سلامت عملیاتی هستند. برای مثال در هنگام شروع شیفت، بکارگیری داشبوردی ساده کهPLC های مشکل‌دار را به رنگ قرمز و موارد پایدار و معمولی را به رنگ سبز نمایش می‌دهد، منجر به تمرکز بهتر بر روی حوزه‌هایی می‌شود که نیازمند هستند. حرکت پرشتابی که به سمت انجام کارهای عملیاتی به

صورت دیجیتالیزه و به هم متصل‌تر وجود دارد باعث افزایش نیاز به وجود نماهایی متمرکز در سطح محیط‌های OT شده است.

۹-۲-۲- اعتبارسنجی دارایی‌ها

سازمان‌ها با قابلیت نظارت کامل بر روی دارایی‌های بخش OT و کنترل آنها، مثل رابط‌های انسان ماشین، ابزارهای ثبت تاریخچه و کنترل‌گرها، می‌توانند با واقعیت موجود در تشکیلات‌شان آشنا شوند. وجود یک منبع کامل متشکل از فهرست دارایی‌ها به ایجاد دید واضح کمک می‌کند. در اختیار داشتن چنین دیدی جهت تشخیص پیکربندی‌های نادرست، آسیب‌پذیری‌ها و سایر نقاط ضعف در کل محیط کنترل صنعتی ضروری است.

در صورت انجام و اجرای صحیح فرایند ایجاد نظارت، باید علاوه بر وجود دارایی‌های مختلف، نسخه، وضعیت میان‌افزار و وضعیت پیکربندی آنها نیز مشخص شود. آگاهی نسبت به اینکه کنترل‌گری با نسخه آسیب‌پذیر یک میان‌افزار کار می‌کند و اینکه آیا فروشنده آن، به‌روزرسانی خاصی برای دستگاه منتشر نموده یا خیر بسیار مهم است.

مالکان دارایی‌ها معمولاً منابع ارزشمند زیادی را صرف بررسی و شناسایی دستی دستگاه‌های متصل به شبکه از جمله سوئیچ‌های شبکه، ایستگاه‌های کاری یا حتی کنترل‌گرهای پردازش می‌کنند. این روش کارایی چندانی نداشته و احتمال بروز خطاهای چشمگیری را هم دارد. جمع‌آوری و به‌روزرسانی خودکار این اطلاعات، وجود یک فهرست دارایی منسجم در سطح کل تشکیلات با قابلیت مقیاس‌پذیری را تضمین می‌کند. همچنین این اطلاعات دنیایی از امکانات مختلف را برای اعتبارسنجی وضعیت دارایی‌ها به ویژه در صورت عدم دسترسی به تیم‌های عملیات در اثر اشتغال فراوان فراهم می‌کنند.

۹-۲-۳- تشخیص و مصورسازی روابط بین دارایی‌ها و مسیرهای ارتباطی

امکان قابلیت نظارت بر روی دارایی‌ها علاوه بر فراهم نمودن اطلاعاتی درباره آنها، داده‌های ارزشمندی را نیز درباره روابط و مسیرهای ارتباطی که در بین‌شان وجود دارند فراهم می‌کند. سازمان‌ها با استفاده از قابلیت نظارت کامل می‌توانند بر روی کانال‌های ارتباطی مدیریت شخص ثالث و OEM نظارت داشته باشند. آن‌ها همچنین اطمینان می‌یابند که این شرکت‌ها به موارد ذکر شده در قرارداد پایبند بوده و مخاطرات غیرضروری برای اکوسیستم ICS ایجاد نمی‌کنند. چنین قابلیت دید و نظارتی شامل نظارت بر روی مسیرهای ارتباطی است که نباید پیامی را به سایر سیستم‌ها ارسال کنند و باید عملیات مشخص را در بازه زمانی تأیید شده انجام دهند. در صورت ارسال فرمان‌های ناگهانی یک ایستگاه کاری به یک کنترل‌گر در

منطقه ۲ در حالی که این ایستگاه کاری فقط باید با دستگاه‌های منطقه ۱ صحبت کند، نیاز به تحقیق و بررسی بیشتر وجود دارد.

ترسیم نقشه دارایی‌ها به نمایش نقاط عطف و تعداد گام‌های بین دارایی‌ها کمک می‌کند. به این ترتیب یک تصویر کلی از وضعیت بخش‌بندی شبکه در اختیار متصدیان و تحلیلگران امنیت قرار می‌دهد تا نقاط مشکل‌آفرین را شناسایی نموده و نحوه حرکت یک مهاجم در شبکه را ارزیابی کنند. این اطلاعات به اعتبارسنجی قوانین فایروال هم کمک می‌نمایند. اگر یک پیمانکار یک مودم سلولی غیرمجاز را برای پشتیبانی از راه دور نصب کرده، باید از این مسئله آگاه باشید. ممکن است این مودم مسیری به یک ایستگاه کاری مهندسی برقرار نموده و مهاجمان با استفاده از آن به یک کنترل‌گر دامنه دسترسی یابند.

این نمایش منطقی علاوه بر ایجاد قابلیت نظارت بر روی فعالیت‌های شبکه، پیکربندی‌های اشتباه و خلأهای موجود در معماری را مشخص می‌کند. مالکان دارایی‌ها با شناسایی چنین خلاءهایی می‌توانند کنترل‌های دفاعی را به صورت پیشگیرانه پیاده‌سازی نمایند. باید با انجام اقدامات ساده مثل نظارت بر روی اکتیودایرکتوری یا ارتباطات راه دور و تقویت محیط یک معماری قابل دفاع ساخت، از اجرای حملات باج‌افزاری پیشگیری کنیم.

۹-۲-٤- تشخیص تهدید

یک رویکرد تشخیص غیرفعال، لزوماً نیازمند نظارت کامل بر روی دارایی‌ها یا خط مبنای رفتار عادی جهت شناسایی تهدیدات فعال در بین دارایی‌ها نیست. همان‌گونه که پیش از این هم اشاره شده، ناهنجاری‌های موجود در وضعیت دارایی‌ها مثل آفلاین شدن یک ایستگاه کاری که عمداً و برای تعمیر غیرفعال شده، لزوماً دلالت بر وجود یک تهدید ندارد. با این وجود شناسایی حملات و مخاطرات امنیتی در دارایی‌هایی که تحت نظارت و کنترل‌مان قرار دارند کار چندان سختی نیست. برای مثال، فایل‌های iso. بزرگ که دارای تشابه نامی زیادی با یک به‌روزرسانی OEM هستند اما مقدار هش آن‌ها با یک فایل مخرب شناخته شده تطبیق دارد، می‌توانند سرنخ‌هایی از وجود فعالیت‌های مخرب باشند.

داشتن قابلیت دید و وجود یک خط مبنا از رفتارها و فهرست دارایی‌ها، به ایجاد سرنخ‌های مهم و حیاتی جهت تسریع در شناسایی تهدیدات کمک می‌کنند. هر یک از این تغییرات می‌توانند به نوبه خود نتایج مثبت یا منفی را به همراه داشته باشند و هر گونه تخدی از خط مبنا لزوماً نشان‌دهنده شرایط پرمخاطره نیست. باز شدن یک پورت دسترسی از راه دور، در بازه زمانی از پیش مشخص شده جهت پشتیبانی از سیستم‌ها توسط فروشنده، لزوماً دلالت بر خطر ندارد اما در صورت امکان برقراری همین پورت با یک سیستم غیرمجاز، شرایط کاملاً متفاوت خواهد بود. اطلاعات محیطی در ترکیب با داده‌های مربوط به رفتار

تهدیدات، زمینه لازم برای تشخیص تغییرات مربوط به تاکتیک‌ها، تکنیک‌ها و روش‌های مهاجمان از تغییرات زیرساختی برنامه‌ریزی شده را فراهم می‌کند.

همه فروشندگان راهکارهایی جامع که منعکس‌کننده چنین نکته مهم و حیاتی باشند ارائه نمی‌دهند. یک قانون تشخیص تهدید که به دلیل وجود جریان ترافیک غرب – شرق فعال شده، زمینه و شرایط کاملاً متفاوتی با ترافیکی دارد. قابلیت نظارت و شناسایی دارایی‌ها یا حتی تشخیص تهدیدات امنیتی به تنهایی کافی نیست. برای ایجاد نظارت کامل بر روی تهدیدات، این دو قابلیت باید با یکدیگر همراه باشند.

۹-۲-۵- تشخیص دارایی‌های مشکل آفرین

متصدیان معمولاً با همه دارایی‌های متصل به فرایندهای اصلی آشنا هستند اما ممکن است نسبت به وجود دارایی‌های مخفی یا مشکل‌آفرینی که محیط را در معرض خطر قرار می‌دهند آگاه نباشند. این مسئله برای شرکت‌هایی که شعبه‌های راه دور یا تشکیلات بزرگ و پیچیده با سطوح امنیت فیزیکی مختلف دارند، مشکل‌آفرین است. این دارایی مخاطره‌آمیز می‌تواند لپ‌تاپ یا یک دستگاه قدیمی از رده خارج شده‌ای مانند یک درایو ذخیره اطلاعات USB خارجی که برای پشتیبان‌گیری استفاده می‌شود که توسط یک تکنسین برای عیب‌یابی و رفع مشکل به شبکه متصل مانده یا دستگاهی مثل دوربین نظارتی باشد که با نیات مخرب مستقر شده‌اند.

متصدیان سیستم‌ها معمولاً اطلاعی درباره وجود چنین تجهیزاتی ندارند. مهاجمان نیز همواره در حال تلاش برای نفوذ به دستگاه‌هایی هستند که به صورت کامل توسط سازمان‌ها شناسایی نشده‌اند.

پیش از ابداع روش‌های خودکار تشخیص دارایی‌ها، روش سنتی برای شناسایی چنین دستگاه‌هایی، مستلزم اجرای یک فرایند بررسی دستی پرزحمت بود. حتی در صورت استفاده از اتوماسیون، بررسی تشکیلات به صورت حضوری و دستی همچنان نقش مهمی در حفاظت از امنیت دارد. البته منابع مورد نیاز برای انجام این کار زیاد است و سازمان‌ها معمولاً این عملیات را به صورت سالیانه، دو بار در سال یا هر سه ماه یک بار انجام می‌دهند. وجود یک روش خودکار جهت تشخیص دارایی‌های مشکل‌آفرین در فاصله بین انجام بررسی‌های دستی تأثیر چشمگیری بر ایمن‌سازی پیوسته محیط‌های OT دارد.

۹-۲-۶- واکنش به حادثه

قابلیت نظارت کامل و به‌روز نسبت به دارایی‌ها، نقش مهمی در کل چرخه واکنش به حادثه دارد. در صورتی که مسئولان واکنش به حادثه فهرست کامل و دقیقی از دارایی‌های موجود در اختیار داشته باشند، به راحتی و در اسرع وقت وجود تهدید و وقوع حادثه را تأیید می‌کنند. در هنگام انجام تحقیقات، قابلیت نظارت کافی بر روی دارایی‌ها تأثیر زیادی در تشخیص گستردگی حادثه و درک کامل سیستم‌های تحت

تأثیر اقدامات مهاجمان دارد. آگاهی نسبت به اینکه یک رابط انسان ماشین هک شده در کدام شعبه و محل قرار دارد، به کاهش هزینه‌ها و تسریع در فرایند جرم‌شناسی کمک می‌کند.

همچنین سازمان‌ها می‌توانند با استفاده از اطلاعاتی که توسط این قابلیت فراهم می‌شوند جهت طراحی و پیاده‌سازی برنامه‌های مقابله با حمله برنامه‌ریزی کنند. در آخرین مراحل واکنش به حادثه این قابلیت نیز به مسئولان اطمینان می‌دهد که تهدید مدنظر به صورت کامل ریشه‌کن شده است.

۹-۲-۷- مقابله با تهدیدات و آسیب‌پذیری‌های حیاتی جدید

آیا می‌توانید به سرعت به این پرسش مدیران اجرایی پاسخ دهید که زیرساخت سازمان شما تحت تأثیر آسیب‌پذیری جدیدی یا تاکتیک‌ها و روش‌های یک گروه جدید قرار دارد یا خیر؟ با استفاده از فهرستی در دسترس و قابل جستجو از دارایی‌های موجود می‌توانید تحقیقات لازم درباره ارتباط تهدیدات جدید با سازمان‌تان را در اسرع وقت انجام دهید.

همچنین با در اختیار داشتن این اطلاعات می‌توانید مشخص نمایید که تجهیزات نیازمند به نصب وصله‌های امنیتی در کدام بخش از سازمان هستند یا در صورت عدم امکان نصب وصله‌های امنیتی، کنترل‌های جبرانی لازم را برای آنها پیاده‌سازی کنید. به این ترتیب علاوه بر تسریع فرایند رسیدگی به ریسک‌های جدید بسیار حیاتی، فرایندهای روزمره مدیریت وصله‌های امنیتی و آسیب‌پذیری‌ها نیز به راحتی انجام می‌شوند. تیم‌های امنیتی در محیط‌های تولیدی باید اطلاعات کاملی از آسیب‌پذیری‌های قابل رفع با وصله‌های امنیتی داشته و برنامه‌ریزی دقیقی درباره رویدادهایی مثل خاموشی سیستم‌ها انجام دهند.

مدیریت آسیب‌پذیری بدون اتوماسیون، منجر به نابودی منابع می‌شود. تیم‌های امنیت سایبری بدون در اختیار داشتن یک دید متمرکز بر روی آسیب‌پذیری‌ها و وجود یک حلقه بسته مثل نصب وصله‌های امنیتی، تغییر پیکربندی و تغییر پورت/پروتکل مسیریابی برای مدیریت کنترل‌هایی که به آسیب‌پذیری‌ها رسیدگی می‌کند، با چالش زیادی مواجه خواهند شد.

۹-۲-۸- تکمیل مدیریت آسیب‌پذیری با تشخیص پیکربندی

تنظیم استانداردهای پیکربندی برای تجهیزات فناوری عملیاتی و پایبندی به این استانداردها کار چندان آسانی نیست. تغییر پیکربندی در یک شبکه صنعتی پویا امری رایج است و عملیات پیگیری و مدیریت لحظه‌ای این تغییرات بسیار سخت می‌باشد.

با امکان دید واضح بر روی دارایی‌ها، عملیات تشخیص تغییرات پیکربندی که منجر به تضعیف زیرساخت‌ها یا حتی نقض قوانین و استانداردها می‌شوند، راحت‌تر انجام می‌شود. این نظارت اطلاعات لازم را برای مدیریت تغییر و تکامل طرح مدیریت دارایی که نقش مهمی در حفظ امنیت و همچنین جامعیت

عملیاتی دارد ایجاد می‌کند. غیرفعال شدن گزارش‌های دسترسی به یک سرور مخصوص مدیریت وصله‌های امنیتی توسط یک مهاجم می‌تواند جریمه‌های سنگینی برای شرکت‌ها به همراه داشته و حتی منجر به ایجاد اختلال در عملیات آنها گردد.

۹-۲-۹- کمک به تولید گزارشات رعایت الزامات قانونی

داشتن دید کامل بر روی دارایی‌ها می‌تواند کمک قابل توجهی به کارمندان بخش امنیت سایبری در زمینه رعایت الزامات و استانداردهای قانونی کند. متصدیان این بخش معمولاً تحت فشار الزامات قانونی قرار دارند تا به صورت منظم کنترل‌های دارایی و امنیتی را به بازرسان گزارش دهند. انجام چنین کاری در سازمان‌ها معمولاً مستلزم اجرای فرایندهای دستی سنگین بوده و حتی ممکن است در کارهای روزمره اختلال ایجاد کند. تشخیص، تحلیل و نگاشت خودکار دارایی‌ها می‌تواند فرایند گزارش‌دهی قانونی را برای کل تیم راحت‌تر نموده و منابع را آزاد کند. اصلاحات امنیتی و عملیاتی نیز با استفاده از روش‌های معنادارتر و مفیدتری انجام می‌شوند.

مدیریت پیکربندی دارایی‌ها شامل تعیین خط مبنای پیکربندی برای دارایی‌های اطلاعاتی، دارایی‌های بخش IT و دارایی‌های OT و همچنین کسب اطمینان از پیکربندی این دارایی‌ها بر اساس خط مبنای تعریف شده است. این اطلاعات به کسب اطمینان از پیکربندی دستگاه‌های مشابه به صورت یکسان کمک می‌کنند اما در صورتی که بعضی از دارایی‌ها منحصربفرد بوده یا دارای پیکربندی‌های متفاوتی باشند، باید معیار پیکربندی در فرایند مدیریت پیکربندی برای دارایی مدنظر در محل استقرار آن مشخص شود و این اطمینان حاصل گردد که پیکربندی وسیله مورد نظر همچنان منطبق با خط مبنای مشخص شده خواهد بود.

۹-۲-۱۰- توجیه سرمایه‌گذاری‌های امنیتی

درک پیچیدگی مجموعه دارایی‌های بخش OT از جمله گام‌های ابتدایی لازم برای ارزیابی ریسک است. آگاهی نسبت به محل و شیوه نصب دارایی‌ها و محدوده کنترل‌های امنیتی مربوط به آنها جهت تشخیص خلأهای موجود در کنترل‌ها و فرایندها ضروری است. ممکن است عواقب و پیامدهای منفی به خطر افتادن یک دارایی مرتبط با عملیات صنعتی یا زیرساخت‌های حیاتی بسیار بیشتر از ایجاد مخاطره برای اکثر دستگاه‌های IT باشد.

با نظارت کامل بر روی دارایی‌ها، به راحتی می‌توانید کمبود کنترل‌های امنیتی را تشخیص داده و سرمایه‌گذاری و طرح‌های آینده را الویت‌بندی کنید. فهرست و نقشه دارایی‌ها یک منبع قابل دسترس و قابل به‌روزرسانی در اختیار تیم‌های امنیتی قرار می‌دهد. تیم‌های امنیتی با استفاده از این اطلاعات می‌توانند

برای ترسیم و تغییر نقشه راه خودشان از آن استفاده کنند. این منبع همچنین می‌تواند شواهد لازم را برای توجیه هزینه‌ها یا تغییرات فرایندها فراهم نماید.

۹-۳- سایر مزایای عملیاتی

مزایای اطلاعاتی که در اثر قابلیت نظارت به دست می‌آیند بسیار فراتر از مواردی هستند که در این مقاله مورد بررسی قرار دادیم. کاهش زمان حل مشکلات، بهبود مراقبت‌های پیشگیرانه به دلیل در اختیار داشتن داده‌های بیشتر و اجرای کارآمد عملیات در حین خاموشی برنامه‌ریزی شده از جمله موارد مهمی هستند که نقش مهمی در سود و زیان شرکت‌ها دارند.

این اطلاعات همچنین برای حوزه‌هایی مثل مدیریت کارایی بسیار مفید می‌باشند. با افزایش قابلیت دید بر روی دارایی‌های بخشOT ، تیم‌های عملیاتی به راحتی می‌توانند حوزه‌های مصرف بیش از حد شبکه را شناسایی نموده و مشکلات را پیش از ایجاد تأثیرات عملیاتی شناسایی کنند. تشخیص سوئیچی که در اثر بار سنگین، بعضی از بسته‌ها را نادیده گرفته و شناسایی وقفه‌های ایجاد شده در فرایند جمع‌آوری داده‌ها کار چندان آسانی نیست. تشکیلات آبی را در نظر بگیرید که به دلیل فعال نشدن اخطار مشکل در دریچه کنترل جریان، آب آلوده را وارد سیستم می‌کند. به طور مشابه، داشتن قابلیت دید به ساده‌سازی شناسایی تأثیر مشکلات دارایی‌ها بر روی فرایندهای عملیاتی مثل تشخیص اینکه آیا یک سیستم نظارت بر گاز آفلاین شده است یا سرورهای زمان شبکه کمک می‌کند.

فصل ۱۰– گروه‌های ثالث بزرگترین نقطه خطر یک سازمان

به طور میانگین سازمان‌ها از محصولات ۲۵۰ تا ۵۰۰ فروشنده شخص ثالث استفاده می‌کنند؛ بنابراین جای تعجب نیست که این مسیر حمله بیشترین بازده را برای هکرها دارد. با این وجود بسیاری از کسب‌وکارها همچنان مخاطرات اشخاص ثالث را جدی نگرفته و آن را یک خطر امنیتی واقعی تلقی نمی‌کنند.

۱۰-۱- اشخاص ثالث نامرئی هستند

اگرچه اشخاص ثالث از جنبه فنی نامرئی نیستند اما سازمان‌ها نظارت محدودی بر روی آنها دارند. حدود ۶۰ درصد از سازمان‌ها دید چندان زیادی نسبت به مجوزهای دسترسی اشخاص ثالث به سیستم‌های حیاتی خودشان نداشته و نیمی از سازمان‌ها نیز حتی نمی‌دانند که چه تعداد اشخاص ثالثی به سیستم‌های آنها دسترسی دارند. فعالیت اشخاص ثالث همچنین به صورت منظم تحت نظارت قرار نمی‌گیرد. در نتیجه برای اقداماتی که در حین دسترسی به اطلاعات و سیستم‌های حیاتی انجام می‌دهند، مسئول دانسته نمی‌شوند.

۱۰-۲- کنترل اشخاص ثالث آسان نیست

کسب‌وکارها معمولاً می‌توانند برای کارمندانی که به داده‌ها، برنامه‌های کاربردی و سیستم‌های حیاتی دسترسی دارند کنترل دسترسی مبتنی بر نقش را پیاده‌سازی کنند. همگام‌سازی کاربران عموماً از طریق یک سیستم اکتیودایرکتوری یا منابع انسانی صورت می‌گیرد که قابلیت اتوماسیون و روان‌سازی فرایند اعطای دسترسی به سیستم‌های مورد نیاز را دارد. فروشندگان شخص ثالث کارمند نیستند و در سیستم‌های داخلی قرار ندارند. در نتیجه مدیریت آنها سخت‌تر است. باید با دسترسی‌های آنها رفتاری متفاوت و دقیق‌تر داشت چون احتمال ایجاد تهدیدات خارجی را به وجود می‌آورند. در صورت عدم ایجاد کنترل‌هایی که بر اساس اصل اعتماد صفر پیاده‌سازی شده باشند، نظارتی بر روی اشخاص ثالث در سیستم‌ها وجود نخواهد داشت.

۱۰-۳- بی‌توجهی به قوانین

به طور میانگین حدود نیمی از سازمان‌ها باور ندارند که اشخاص ثالث آنها از قوانین گزارش رخنه اطلاعاتی در صنعت خودشان آگاه هستند. حدود ۶۰ درصد نیز به عملکرد اشخاص ثالث برای پیروی از قوانین حریم خصوصی و امنیت مرتبط با سازمان خودشان امتیاز کمی می‌دهند. در حوزه بهداشت و درمان، مقرراتی مثل HIPAA وجود دارند که بر اساس این قوانین اشخاص ثالث مسئول نقض مقررات هستند اما

تا زمانی که قوانین مشابهی برای سایر صنایع پیاده‌سازی و اجرا نشود، اشخاص ثالث همچنان یک تهدید قانونی و امنیتی مهم برای کسب‌وکارها خواهند بود.

۱۰-٤- ضعف در مدیریت اشخاص ثالث

حدود ۷۰ درصد از شرکت‌کنندگان نظرسنجی اخیر Ponemon اعلام کرده‌اند که مدیریت مجوزها و دسترسی‌های راه دور اشخاص ثالث کار سختی است و منابع داخلی را تخلیه می‌کند. سازمان‌ها معمولاً نیرو یا ظرفیت لازم برای مدیریت اشخاص ثالث را ندارند تا یک تیم مدیریت ریسک کامل مخصوص رسیدگی به اشخاص ثالث راه‌اندازی کنند؛ بنابراین دسترسی‌های راه دور و مجوزهای اشخاص ثالث به خوبی مدیریت نشده یا حتی اصلاً مدیریت نمی‌گردد. سازمان‌ها برای حفظ امنیت شبکه و سیستم‌های خودشان متکی بر روی اعتبار اشخاص ثالث یا قراردادها هستند که البته این اقدام به تنهایی کافی نیست.

۱۰-٥- اشخاص ثالث دری به دنیای بیرون هستند

دسترسی اشخاص ثالث، دری برای ورود دیگران به سازمان و دسترسی به اطلاعات، شبکه‌ها و سیستم‌های حیاتی است. سازمان‌ها معمولاً بر اساس معماری قلعه و خندق ساخته شده‌اند که از آنها در برابر همه افراد خارجی حفاظت می‌کند. این سازوکار ظاهراً عملکرد مناسبی دارد اما در مقابل افرادی که داخل سازمان هستند چندان قوی نیست؛ بنابراین اگر هکری از دسترسی‌های یک شخص ثالث برای هک شرکت شما استفاده کند، به همه درها و دارایی‌های حیاتی که سعی در حفاظت از آنها دارید دسترسی خواهد داشت.

هکرها از دسترسی‌های راه دور شخص ثالث سوءاستفاده می‌کنند. اگر خطر شخص ثالث را جدی نگیرید، دیر یا زود سازمان شما هم باید با عواقب حملات سایبری مواجه شود. با پیاده‌سازی استراتژی‌های مدیریت دسترسی‌های حیاتی، رویکرد اعتماد صفر و توجه به واقعیت تهدیدات شخص ثالث می‌توانید برای مقابله با این مخاطرات آماده شوید.

۱۰-٦- پنج تهدید برتر سایبری

مرکز امنیت اینترنتی پنج حمله اصلی را که سازمان‌ها باید از آنها حفاظت شوند را از طریق Verizon DBIRو منابع دیگر شناسایی کرد:

۱. بدافزار انواع مختلفی از بدافزار وجود دارد و بسیاری از سازمان‌ها متوجه حملات آنها در زمان‌های مختلف با انواع مختلفی می‌شوند. طبقDBIR ، فعال‌ترین انواع بدافزارها امروزه با عنوان dumpers

passwordشناخته می‌شوند که برای سرقت اطلاعات مورد استفاده قرار می‌گیرند. ایمیل‌های فیشینگ و نصب مستقیم رایج‌ترین روش‌های انتشار این نوع بدافزارها هستند. دانلود backdoors) و (key loggers نیز از تهدیدات بدافزاری برجسته هستند.

۲. هک کردن بیش از ۸۰٪ موارد نقض اطلاعات تأیید شده از طریق هک، از روش‌های brute force یا استفاده از مدارک گم‌شده یا به سرقت رفته است. وکتور اصلی حمله از طریق برنامه‌های تحت وب است که به دلیل افزایش محبوبیت برنامه‌های ابری، بخشی از آن در حال افزایش است. بهره‌برداری از آسیب پذیری، درهای پشتی نیز از مهمترین تکنیک‌های هک هستند.

۳. استفاده از امتیاز داخلی و سوءاستفاده در حالی که مهاجمان خارجی عموماً نسبت به خودی‌ها تهدید بزرگتری به شمار می‌روند، کاربران دارای امتیاز هنوز هم ریسک قابل توجهی را به خود اختصاص می‌دهند. DBIR 2020 به کاهش تعداد حملات داخلی از سال گذشته تا کنون اشاره کرد. با این حال، تشخیص این حوادث بسیار دشوار است و زمانی که به طور هوشمندانه پنهان شده‌باشد، می‌تواند برای مدت طولانی ادامه یابد. همچنین، سواستفاده افراد از منابع یا سواستفاده از امتیازاتی که دارند می‌تواند منجر به افشای ناخواسته اطلاعات شود.

٤. نفوذهای هدفمند جاسوسی سایبری همچنان یک نگرانی بزرگ است، اگرچه به نظر می‌رسد اکثر حوادث از بازیگران تحت حمایت دولت به سوی افرادی که صرفاً منافع مالی می‌طلبند دور می‌شود. نفوذهای هدفمند با هک عمومی فرق می‌کند زیرا مرتکبان سخت تلاش خواهند کرد تا شناسایی نشوند و ممکن است با ادامه تمرکز بر قربانی خود، رویکرد خود را تغییر دهند.

٥. باج افزارها نوعی بدافزار هستند که می‌بایست توجه خاصی به آن داشت. باج افزار سومین نوع رایج در بدافزارها است. ابزار احراز هویت یا اعتبارسنجی نیز ممکن است در حمله باج افزار به خطر افتد. خودکارسازی حملات از طریق سرویس‌های آنلاین بدان معنی است که باج افزار همچنان یک مشکل رو به رشد خواهد ماند.

۱۰-۷- تکنیک‌ها و تاکتیک‌های حمله

حفاظت از یک سازمان دربرابر حمله به موارد دیگری بیش از اطلاع از شایع‌ترین تهدیدات سایبری نیاز دارد. هر نوع حمله از یک سری تاکتیک پیروی می‌کند (مراحل حمله). تکنیک‌های زیادی وجود دارد که مهاجم می‌تواند در هر مرحله از آنها استفاده کند.

۱۰-۸- حفاظت در برابر تهدیدات جدید

البته دانستن انواع حمله، تاکتیک‌ها و تکنیک‌ها فقط آغاز کار است. سؤال این است که در مورد آن‌ها چه باید کرد؟ مرکز امنیت اینترنتی برای کمک به سازمان‌ها در طول مسیر امنیت سایبری خود، از اطلاعات موجود در DBIR و ATT & CK برای ایجاد مدل دفاعی جامع استفاده کرد.

CDM انواع مهم حمله را در DBIR شناسایی می‌کند و آنها را با تکنیک‌های مورد نیاز برای اجرای تاکتیک‌های قابل استفاده مطابقت می‌دهد. سپس یک گام فراتر می‌رود تا نقشه‌ای از تدابیر حفاظتی یافت شده در برابر تنکنیکهای بکاررفته در هر حمله در کنترل‌های CIS و مقدار ارزش امنیت اجرای تدابیر حفاظتی را ترسیم کند.

CIS Controlsیک مجموعه تدابیر حفاظتی اولویت بندی شده و تجویزی هستند که رایج‌ترین حملات سایبری علیه سیستم‌ها و شبکه‌ها را کاهش می‌دهد. کنترل‌های CIS بیشتر در سه گروه پیاده سازی سازماندهی می‌شوند تا به سازمانها در تصمیم‌گیری درباره اینکه کدام یک از تدابیرحفاظتی بیشترین ارزش را میسر می‌کنند، کمک کنند. این امر با توجه به اندازه و ماهیت سازمان و همچنین میزان همراهی آنها با برنامه امنیت سایبری تعیین می‌شود.

۱۰-۹- پیاده‌سازی، اتوماسیون و ارزیابی

امروزه ماهیت پیچیده محیط‌های فن‌آوری اطلاعات نیازمند راه‌حل‌های پیشرفته برای اجرا و ارزیابی است. پیاده‌سازی را می‌توان تا حد زیادی از طریق استفاده از ابزارهای خودکار برای ارزیابی و ارتقا از راه دور نقاط مهم انجام داد.

CIS-CAT Pro Assessorیکی از این ابزارهاست. این ابزار با اسکن کردن تنظیمات پیکربندی سیستم هدف و گزارش انطباق سیستم با معیار CIS مربوطه، می‌تواند در بررسی پیکربندی ساعت‌ها صرفه‌جویی کند.

علاوه بر این، ابزار خود ارزیابی CIS مزایای بسیاری را برای ردیابی اجرای کنترل‌هایCIS فراهم می‌کند که فراتر از یک صفحه گسترده ساده است. CIS CSAT اکنون در نسخه "on premise" با گزینه‌های پیشرفته برای تیم‌ها، به نام CIS CSAT Pro در دسترس است. این ابزارها و موارد دیگر از طریق عضویت در CIS SecureSuite در دسترس هستند.

فصل ۱۱– راهکار جامع در زمان افزایش تهدیدات سایبری

با توجه به پیشرفت فناوری و توسعه ابزارهای هک و افزایش تهدیدات سایبری توسط مجرمان، بدیهی است که مخاطرات امنیتی در گذر زمان تغییر می‌کنند؛ بنابراین باید پیش از هر چیز بین تهدیدات کنونی و مخاطراتی که از گذشته وجود دارند توازن برقرار شود. همچنین باید تدابیر مورد نیاز برای مقابله با تهدیدات جدید و پیامدهای ناشی از آنها و تأمین هزینه‌های مربوط به راهکارهای دفاعی جدید ایجاد گردند.

از طرفی ممکن است سطح مخاطره تهدیدات امنیتی احتمالی موجود در یک سازمان از حالت عادی بالاتر باشد. در چنین شرایطی سطح هشدار نیز باید تشدید یافته و قابلیت‌های زیر را ایجاد کند:

- اولویت‌بندی اقدامات لازم؛
- تقویت موقت یا دائم سازوکارهای دفاعی؛
- ایجاد شرایطی که منجر به پیشگیری از حملات سایبری در زمان‌هایی شود که احتمال وقوع‌شان بسیار بالاست؛
- ایجاد تأثیرات مثبت در بازیابی محیط به شرایط پیش از حمله در اسرع وقت.

در این مطلب از فراست عواملی که باعث ایجاد تغییر در مخاطرات امنیتی می‌شوند و اقداماتی که سازمان‌ها در مواجه با حملات سایبری باید انجام دهند را مورد بررسی قرار می‌دهیم.

۱۱-۱- عوامل تأثیرگذار بر روی مخاطرات سایبری یک سازمان

ظهور اطلاعات جدید مبنی بر تشدید تهدیدات سایبری توسط تیم امنیتی یک سازمان می‌تواند منجر به تغییر دیدگاه آن سازمان نسبت به تهدیدات شود.

افزایش مخاطرات امنیتی ممکن است ناشی از تقویت موقت قابلیت‌های مهاجمان باشد. برای مثال شناسایی یک آسیب‌پذیری روز صفر در یک سرویس پرکاربرد می‌تواند دلالت بر سوءاستفاده پیوسته مهاجمان از این آسیب‌پذیری داشته باشد. چنین تهدیدی همچنین ممکن است مخصوص یک سازمان، بخش یا حتی کشور خاصی باشد که از تنش‌های ژئوپلیتیک یا هکتیویسم ناشی شده‌اند.

بنابراین سازمان‌های بزرگ و کوچک باید اقدامات لازم برای واکنش سریع و به‌موقع به رویدادهای مخاطره‌آمیز را انجام دهند. کسب‌وکارها معمولاً نمی‌توانند تأثیر خاصی بر روی سطح حمله داشته باشند. همچنین مهاجمان همواره در حال تلاش برای سوءاستفاده از آسیب‌پذیری‌های شناخته شده، پیکربندی‌های اشتباه و حمله از طریق اعتبارنامه‌های کاربری (مثل اسپری کردن کلمه عبور، سوءاستفاده از رمزهای لو

رفته یا استفاده مجدد از توکن احراز هویت) هستند؛ بنابراین تیم‌های امنیتی باید با تمرکز بر روی کاهش آسیب‌پذیری از میزان پیامدهای منفی حملات سایبری نیز بکاهند. حذف قابلیت این افراد برای استفاده از چنین تکنیک‌هایی می‌تواند ریسک مخاطرات سایبری را به صورت قابل توجهی کاهش دهد.

۱۱-۲- اقدامات قابل انجام

ابتدا کلیه سازمان‌ها و کسب‌وکارها باید از وجود اصول و پایه‌های امنیتی و کنترل‌های بهداشت سایبری جهت حفاظت از دستگاه‌ها، شبکه‌ها و سیستم‌ها اطمینان یابند. انجام اقدامات زیر به سازمان‌ها برای ارزیابی و سنجش میزان امنیت محیط به‌ویژه در زمان تشدید تهدیدات سایبری بسیار حیاتی کمک می‌کند.

البته سازمان‌ها معمولاً نمی‌توانند در مدت کوتاه تغییرات گسترده‌ای را در سیستم‌های‌شان ایجاد نمایند ولی در هر صورت باید تلاش کنند تا اقدامات زیر را به ترتیب اولویت انجام دهند.

۱۱-۲-۱- بررسی وصله‌های امنیتی سیستم‌ها

- اطمینان یابید که کامپیوترها، لپ‌تاپ‌ها، دستگاه‌های همراه، نرم‌افزارهای شخص ثالث مثل مرورگرها و سایر ابزارهای کاربردی به روزرسانی شده و در صورت امکان قابلیت به روزرسانی‌های خودکار را فعال کنید.
- بررسی‌های لازم جهت آگاهی از وجود وصله‌های امنیتی میان‌افزارهای دستگاه‌های سازمان را انجام دهید. ممکن است شیوه نصب این وصله‌های امنیتی با روش نصب به‌روزرسانی نرم‌افزار متفاوت باشد.
- مطمئن شوید که وصله‌های امنیتی برای سرویس‌هایی که با اینترنت در تماس هستند نصب شده باشند. آسیب‌پذیری‌های موجود در این سرویس‌ها می‌توانند منجر به ایجاد مخاطرات غیرقابل مدیریت شوند.
- همواره از به‌روزرسانی سیستم‌های کلیدی کسب‌وکارتان اطمینان یابید. باید تدابیر امنیتی لازم برای مقابله با آسیب‌پذیری‌های رفع نشده ایجاد شوند.
- انگیزه‌های تجاری که در صورت عدم نصب وصله‌های امنیتی و با توجه به تشدید تهدیدات به وجود می‌آیند را بررسی کنید.

۱۱-۲-۲- اعتبارسنجی کنترل‌های دسترسی

- کارمندان باید کلمات عبور منحصربفردی را برای سیستم‌های کاری‌شان تنظیم نموده و از بکارگیری رمزهای مشترک با سیستم‌ها و حساب‌های کاربری غیرکاری جداً خودداری کنند. توصیه می‌شود که افراد بهتر است از کلمات عبور قوی و متمایز برای هر سیستم و حساب کاربری استفاده کنند.
- کنترل‌های کاربری را بازبینی نموده و حساب‌های قدیمی یا بدون استفاده را حذف کنید. احراز هویت دو یا چند مرحله‌ای را فعال و بررسی کنید که این قابلیت در کلیه سیستم‌ها و حساب‌های کاربری و متناسب با سیاست‌های کاری‌تان فعال است. از پیکربندی صحیح آن نیز اطمینان یابید.
- حساب‌هایی که دارای سطح دسترسی‌های مدیریتی یا ممتاز هستند را با دقت بازبینی نموده و حساب‌های کاربری قدیمی بدون استفاده یا پیکربندی نشده را حذف کنید. مدیریت این حساب‌ها باید به روشی اصولی و صحیح باشد و در صورت امکان، احراز هویت چند مرحله‌ای را هم فعال کنید. این دسترسی‌های ممتاز معمولاً مرتبط با مدیر سیستم و همچنین دسترسی به سایر اطلاعات یا منابع حساس هستند؛ پس این منابع نیز باید حفظ گردند.
- جهت درک مخاطرات امنیتی موجود در سیستم‌ها و آگاهی کامل از آنها، معماری کلی مدیریت سیستم را مطالعه کنید.

۱۱-۲-۳- اطمینان از عملکرد سازوکارهای دفاعی

برای اطمینان از عملکرد دفاعی سیستم؛ موارد زیر را بررسی کنید:

- نصب نرم‌افزار آنتی‌ویروس؛
- بررسی پیوسته فعالیت آنتی‌ویروس بر روی همه سیستم‌ها و همچنین به روزبودن آن؛
- شیوه عملکرد قوانین فایروال به ویژه قوانین موقتی که ممکن است بیش از طول عمر مورد انتظار در سیستم باقی بمانند.

۱۱-۲-٤- ثبت گزارش وقایع و نظارت

- گزارش‌های موجود، محل ذخیره آنها و مدت زمان نگهداری‌شان را بازبینی کنید. گزارش‌های کلیدی را تحت نظارت داشته و گزارش‌های آنتی‌ویروس را بررسی نمایید. در صورت امکان ماهیانه اطمینان حاصل کنید که همه گزارش‌های لازم ذخیره و حفظ می‌شوند.

۱۱-۲-۵- بازبینی نسخه‌های پشتیبان

- بررسی کنید که نسخه‌های پشتیبان به درستی ایجاد می‌شوند. این نسخه‌های پشتیبان را ارزیابی نموده و اطمینان یابید که فرایند بازیابی‌شان قابل درک و آسان باشد.
- بررسی کنید که آیا فایل‌های پشتیبان دارای نسخه‌های آفلاین هستند یا خیر؛ همچنین این نسخه‌ها باید به‌روز بوده و در صورت وقوع حملاتی که منجر به از دست رفتن داده‌ها یا پیکربندی سیستم‌ها می‌شوند قابل استفاده باشند.
- باید از وضعیت سیستم‌ها و اعتبارنامه‌های کاربری مهم خارجی (مثل کلیدهای خصوصی و توکن‌های دسترسی) نیز نسخه‌های پشتیبان تهیه شود.

۱۱-۲-۶- برنامه‌ریزی‌های لازم برای حادثه را انجام دهید

- طرح واکنش به حادثه شما، اطلاعات تماس و مسیرهای ارتقای سطح دسترسی باید به‌روز باشد.
- اطلاعات مورد نیاز درباره شخصی که اختیار انجام تصمیم‌گیری‌های کلیدی را در طرح واکنش به حادثه و به‌ویژه در زمان‌هایی خارج از ساعات کاری برعهده دارد به دست آورده و بررسی‌های لازم را در این زمینه انجام دهید.
- از در دسترس بودن طرح واکنش به حادثه و سازوکارهای ارتباطی مورد استفاده آن اطمینان یابید حتی اگر سیستم‌های کاری از دسترس خارج شدند.

۱۱-۲-۷- بررسی ردپای موجود در اینترنت

- بررسی کنید که رکوردهای ردپای اینترنتی سازمان درست و به روز باشند. همچنین اطمینان یابید که داده‌های ثبت دامنه به صورت امن نگهداری می‌شوند و اعطای نمایندگی و اختیاری نیز بر اساس انتظار انجام می‌گردد.
- یک اسکن آسیب‌پذیری خارجی از کل ردپای اینترنتی‌تان انجام داده و بررسی کنید که کلیه وصله‌های امنیتی لازم نصب شده باشند.

۱۱-۲-۸- واکنش به فیشینگ

- آموزش‌های لازم درباره شیوه گزارش‌دهی ایمیل‌های فیشینگ را به کارمندان‌تان داده و طرح رسیدگی به این گزارش‌ها را هم ایجاد کنید.

۱۱-۲-۹- دسترسی‌های شخص ثالث

- باید درک و آگاهی کامل نسبت به دسترسی‌های سازمان‌های شخص ثالث به دستگاه‌ها و شبکه‌های خود داشته و دسترسی‌های غیرضروری را حذف کنید. همچنین باید اصول و قوانین امنیتی شرکت شخص ثالث همکار را بدانید.

۱۱-۲-۱۰- جلب همکاری سایر تیم‌های سازمان

- توجه سایر بخش‌های سازمان به مخاطرات امنیتی نقش بسزایی در کاهش تهدیدات و به صورت کلی انجام موفقیت‌آمیز اقدامات بالا دارد؛ بنابراین سازمان‌ها باید امکاناتی را جهت جلب نظر کلیه کارکنان سازمان به‌ویژه در شرایطی که تهدیدات تشدید می‌یابند ایجاد کنند.
- اطمینان یابید که همکاران‌تان در سایر حوزه‌ها، پیامدهای منفی احتمالی تهدیدات بر روی وظایف و کارهای تیم خودشان را درک می‌کنند. همه باید با شیوه گزارش‌دهی رویدادهای امنیتی مشکوک و همچنین میزان اهمیت ارسال گزارش آشنا باشند.

۱۱-۳- اقدامات پیشرفته

کلیه سازمان‌های بزرگ و کوچک باید جهت پیاده‌سازی تدابیر امنیتی مورد نیاز، همه اقدامات ذکر شده در این مطلب را انجام دهند. سازمان‌ها و قانون گذارانی که از فریم‌ورک ارزیابی سایبری برای درک مخاطرات امنیتی استفاده می‌کنند باید بدانند که CAF شامل راهنمایی‌هایی درباره این اقدامات است؛ بنابراین شرکت‌هایی که توجه چندانی به این موارد ندارند باید در صورت تشدید تهدیدات، بلافاصله در تصمیمات‌شان تجدید نظر نمایند. بنا بر توصیه کارشناسان امنیتی، کسب‌وکارهایی که از منابع و اطلاعات حساس بیشتری استفاده می‌کنند باید اقدامات زیر را هم انجام دهند:

- اگر سازمان قصد توسعه تدریجی طرح‌های امنیت سایبری خود را دارد باید بررسی کند که آیا نیازی به پیاده‌سازی سریع تدابیر امنیتی کلیدی برای شرایط حساس ناشی از تشدید تهدیدات سایبری هست یا خیر. ممکن است انجام چنین کاری مستلزم تغییر اولویت‌های شما در زمینه تخصیص منابع یا سرمایه باشد.
- هیچ سیستم یا سرویسی در دنیای فناوری بدون مخاطرات نبوده و سازمان‌های بالغ سعی می‌کنند تصمیمات مبتنی بر ریسک آگاهانه و متعادلی بگیرند. وقتی تهدیدی شدت می‌یابد، سازمان‌ها باید تصمیمات مبتنی بر ریسک کلیدی‌شان را بازبینی نموده و بررسی کنند که آیا

مایل به ادامه تحمل چنین مخاطراتی هستند یا باید اقداماتی در راستای کاهش و رفع آنها انجام دهند.

- ممکن است بعضی از عملکردهای سیستمی مثل مبادله داده‌ها با شبکه‌های غیر قابل اطمینان منجر به افزایش سطح مخاطرات سایبری شود. سازمان‌های بزرگ که معمولاً سازوکارهایی جهت ارزیابی، آزمودن و اعمال وصله‌های امنیتی در مقیاس عظیم دارند باید بسنجند که آیا پذیرش کاهش موقت سطح یک عملکرد جهت کاهش تهدیدات سایبری قابل قبول است یا خیر. وقتی تهدیدی شدت می‌گیرد، ممکن است سازمان شما مایل به در پیش گرفتن روشی تهاجمی‌تر برای رفع آسیب‌پذیری‌ها باشد.
- در چنین زمان‌هایی سازمان‌ها باید تغییرات سیستمی قابل توجهی که ارتباطی به امنیت ندارند را به تعویق بیندازند.
- اگر یک تیم امنیت عملیاتی یا مرکز عملیات امنیتی دارید، بهتر است برای افزایش ساعت‌های عملیاتی برنامه‌ریزی کنید یا در صورت وقوع حادثه امنیتی آمادگی لازم جهت افزایش مقیاس سریع عملیات را داشته باشید.
- اگر سیستم‌هایی دارید که قابلیت انجام کارهای خودکار یا ارسال اعلان بر اساس هوش تهدید را دارند، بهتر است فیدهای تهدیدی را تهیه کنید که در زمان تشدید تهدیدات، اطلاعات لازم را در اختیار شما قرار می‌دهند.

فصل ۱۲– بیومتریک، مزایا و معایب

در حال حاضر با توجه به پیشرفت فناوری‌های مورد استفاده توسط هکرها و افزایش حملات سایبری، کلمه‌های عبور معمولی که متشکل از یک رشته از کاراکترها، حروف و اعداد هستند نه تنها امن نبوده بلکه حتی مجرمان سایبری به راحتی می‌توانند به آنها دسترسی یابند.

با وجود اینکه کاربران امکان استفاده از یک رمز عبور مشابه و ساده برای چندین حساب کاربری را دارند یا می‌توانند از یک برنامه مدیریت رمز عبور برای تعیین و انتخاب کلمه‌های عبور پیچیده استفاده نموده و هر چند وقت یکبار آن‌ها را تغییر دهند، اما توصیه‌های کارشناسان امنیتی به افراد این است که به جای انتخاب رشته‌ای تصادفی از کاراکترها، از فناوری‌های جدید مانند بیومتریک که برای هر فرد کاملاً منحصر به فرد است و امکان هک آن به سادگی وجود ندارد، برای حساب‌های کاربری‌شان استفاده کنند.

بر اساس تحقیقات انجام شده از هر ده نفر، یک نفر گزارش هک حداقل یکی از حساب‌های خود را داده بود. همچنین ۸۰ درصد از قربانیان این کلاهبرداری‌ها همواره از اینکه دوباره در دام بیفتند، احساس ترس داشتند.

حتی مشاغل و سازمان‌ها نیز از این حملات در امان نیستند. بر اساس گزارش‌های دریافتی از شرکت‌های انگلیسی، این کلاهبرداری‌ها حدود ۲۰ هزار پوند ضرر مالی برای بسیاری از شرکت‌ها و کسب‌وکارشان به بار آورده‌اند. این سازمان‌ها علاوه بر اینکه ناچار به خسارت‌های مالی سنگین شدند، اعتمادشان در بین مشتریان خود را از دست داده و حدود یک چهارم از قربانیان این کلاهبرداری‌ها اعلام کردند که پس از وقوع چنین حوادثی، مبادلات و معاملات تجاری خود با کسب‌وکار مربوطه را متوقف نمودند.

در پی افزایش حملات افشای رمز عبور و دسترسی مهاجمان به داده‌های حساس سازمان‌ها و همچنین بر اساس توصیه‌های پی در پی کارشناسان امنیتی، شرکت‌ها به منظور حفاظت از اطلاعات و سیستم‌هایشان به روش‌های امنیتی و نوین بیومتریک روی آوردند.

۱۲-۱- بیومتریک چیست و چگونه هک می‌شوند؟

تکنولوژی بیومتریک به روش‌های خودکار تشخیص یا تأیید هویت یک شخص زنده از طریق اندازه‌گیری مشخصه‌های فیزیولوژیکی یا رفتاری وی اطلاق می‌شود؛ بدین ترتیب بیومتریک یک مجموعه فناوری محسوب می‌گردد.

فناوری بیومتریک که در فارسی به آن فناوری زیست سنجی گویند، فناوری است که ویژگی‌ها و خصایص یکتا و منحصر به فرد یک انسان را اندازه گیری می‌کند. این فناوری برای احراز هویت و کنترل دسترسی

به کار می‌رود. کاربرد فناوری بیومتریک در فرودگاه‌ها، ساعت‌های حضور و غیاب، ورودی‌های ساختمان و قفل‌های هوشمند در ساختمان‌های هوشمند، خودروهای جدید، پایگاه‌های اهدای خون، مدارس، مراکز داده و بسیاری از مکان‌های دیگر است. از جمله پارامترهای مهم برای بیومتریک اثر انگشت، هندسه کف دست، قرنیه چشم، شبکیه چشم، صورت و الگوری راه رفتن است. بیومتریک به دلیل دنیای دیجیتال، محافظت از داده‌های محرمانه، احراز هویت افراد برای استفاده از دستگاه مسیر رشد بالایی را در این زمان پیش رو دارد. در بسیاری از نوشتارها اشاره به این شده است که بیومتریک مناسب‌تر از رمز عبور بوده و بر اساس یک گزارش میدانی، ۴۸٪ افراد بر این باورند که بیومتریک نسبت به رمز عبور امن‌تر ماست.

۱۲-۲- احراز هویت بیومتریک چیست؟

به بیانی ساده احراز هویت بیومتریک تأیید هویت شما با اندازه‌گیری ویژگی‌های منحصر به فرد بدن شما می‌باشد که پس از شناسایی، شما را به سرویس، اپلیکیشن، سامانه و... وارد می‌کند. دلیل پیچیدگی این تکنولوژی در آن نهان است، حال بیایید ببینیم این تکنولوژی چگونه کار می‌کند. احراز هویت بیومتریک یک مرحله جلوتر رفته و از اطلاعات افراد برای مقایسه با یک پایگاه داده استفاده می‌کند و آنها را به یک سرویس وارد می‌کند.

به این موضوع این گونه نگاه کنید: شناسایی بیومتریک مانند فردی است که با چشم نیمه باز از طریق روزنه در می‌خواهد به ۲ نفر که زنگ زده‌اند، نگاه کند. او بر اساس قد، رنگ مو، رنگ چشم و... تصمیم می‌گیرد که کدام‌یک از آنها دوست است. احراز هویت بیومتریک، همان فردی است که با چشم نیمه باز از طریق روزنه در می‌خواهد ببیند چه کسی به دیدار او رفته است. اگر دوست باشد، به او اجازه ورود می‌دهد.

موضوعی که ما در این مقاله پوشش می‌دهیم توضیح گسترده‌ای از احراز هویت بیومتریک، یک تکنولوژی جذاب که در حال حاضر به شکل قابل توجهی پذیرفته شده است و پتانسیل گسترش در آینده را دارد، می‌باشد.

۱۲-۲-۱- لیست محتوا

- احراز هویت بیومتریک چگونه کار می‌کند؟
- روش‌های احراز هویت بیومتریک و نحوه کار آنها:
  - ✓ اسکنر اثرانگشت و نحوه ذخیره‌سازی اطلاعات توسط آن
  - ✓ تکنولوژی بیومتریک سیستم تشخیص چهره
  - ✓ اسکنر چشم

- ✓ شناسایی متکلم

- سایر فناوری‌های بیومتریک
- مزایا و معایب اراز هویت بیومتریک
- روش‌های هک کردن
- چگونه تلفن هوشمند / لپ‌تاپ را با اسکنر اثرانگشت ایمن

احراز هویت بیومتریک با مقایسه دو مجموعه داده کار می‌کند: اولین مورد توسط صاحب دستگاه از پیش تعیین شده است، در حالی‌که دومین داده به بازدید کننده دستگاه تعلق دارد. اگر دو داده تقریباً یکسان باشند، دستگاه می‌داند که "بازدیدکننده" و "صاحب دستگاه" یک نفرند و به شخص اجازه دسترسی می‌دهد.

۱۲-۳- احراز هویت بیومتریک چگونه کار می‌کند؟

نکته مهم این است که تطبیق بین دو مجموعه داده تقریباً یکسان است اما دقیقاً یکسان نیست؛ زیرا ممکن است مجموعه داده بیومتریک ۱۰۰٪ مطابقت نداشته باشند. به عنوان مثال، ممکن است انگشت ما کمی عرق کرده و خیس، کثیف و یا کمی زخمی باشد و در اثر آنها مدل اثر انگشت تغییر کند.

طراحی فرایند به‌طوری که نیازی به تطبیق دقیق نداشته باشد احتمال خطا و در عین حال شانس اینکه اثر انگشت جعلی، صحیح در نظر گرفته شود را افزایش می‌دهد.

۱۲-٤- روش‌های احراز هویت بیومتریک و نحوه کار آنها

چندین روش احراز هویت برای شناسایی کاربران سامانه‌ها وجود دارد که در ادامه به آنها اشاره‌شده است.

۱۲-٤-۱- اسکنر اثر انگشت و نحوه ذخیره‌سازی اطلاعات توسط آن

سه نوع اسکنر اثر انگشت وجود دارد: نوری، خازنی و اولتراسونیک (امواج فراصوتی).

- اسکنر نوری یک عکس از انگشت می‌گیرد، مدل اثرانگشت را شناسایی می‌کند، سپس آن را به یک کد شناسایی تبدیل می‌کند.
- اسکنر خازنی با اندازه‌گیری سیگنال‌های الکتریکی ارسال‌شده از انگشت به اسکنر، کار می‌کند. برآمدگی‌های انگشت به‌طور مستقیم با اسکنر در تماس قرار می‌گیرند، جریان الکتریکی را

ارسال می‌کنند، درحالی‌که شیارهای اثرانگشت، شکاف‌های هوایی ایجاد می‌کنند. یک اسکنر خازنی اساساً این نقاط تماس و شیارهای هوایی را که منجر به یک مدل کاملاً منحصربه‌فرد می‌شوند به تصویر می‌کشد. این نمونه از اسکنرها درگوشی‌های هوشمند و لپ‌تاپ‌ها استفاده می‌شوند.

- اسکنر اولتراسونیک که در جدیدترین نسل از تلفن‌های هوشمند بکار برده خواهد شد، امواج فراصوتی را منتشر می‌کند که دوباره به اسکنر بازمی‌گردند و مانند اسکنر خازنی، یک مدل منحصر از انگشت همان فرد را ارائه می‌دهد.

۱-۱-۴-۱۲- اثر انگشت شما چگونه ذخیره می‌شود؟

گوگل و اپل هر دو، اثر انگشت شما را بر روی دستگاه خود شما ذخیره می‌کنند و هیچ نسخه‌ای از آن را در سرورهای خود کپی نمی‌کنند.

شناساگر اثر انگشت اپل تصویر واقعی اثرانگشت شما را ذخیره نمی‌کند بلکه یک نمایش ریاضی از آن را ذخیره می‌کند؛ بنابراین حتی اگر یک هکر مخرب به این نمایش ریاضی دست یابد، نمی‌تواند آن را طوری طراحی کند تا یک عکس واقعی از اثر انگشت شما را نشان دهد. علاوه بر این، داده‌های اثر انگشت شما رمزگذاری می‌شوند.

همان‌طور که یک محقق امنیتی اشاره کرده است، اگرچه شناساگر اثر انگشت را می‌توان هک کرد ولی این روش هنوز هم یک روش بسیار امن برای احراز هویت بیومتریک است. کسی که می‌خواهد یک گوشی اپل با شناساگر اثر انگشت را هک کند، به یک کپی بسیار عالی از اثرانگشت شخص نیاز دارد تا به تلفن او دسترسی یابد، به همین دلیل این روش با سرقت یک رمز عبور، کاملاً متفاوت است.

حتی سیستم‌عامل دستگاه هم نمی‌تواند مستقیماً به داده‌های اثر انگشت دسترسی پیدا کند و نسبت به سایر برنامه‌ها دسترسی بسیار کمتری دارد. در عوض، یک نرم‌افزار امنیتی "gatekeeper" باقابلیت تضمین‌کننده امنیت یک جلسه وجود دارد که بین داده‌های اثر انگشت و برنامه‌ای که اسکن اثر انگشت را انجام می‌دهد، قرار می‌گیرد.

"Gatekeeper"فن‌آوری جدید امنیتی اپل است که هم‌زمان با "Mountain Lion" منتشر می‌شود. با این فن‌آوری اپل به شما اجازه می‌دهد برنامه‌های تولیدکنندگان مورد تأیید اپل را نیز در کنار برنامه‌های موجود در Mac Store نصب کنید و درصورتی‌که این برنامه در اجرا با مشکل حادی مواجه شود، اپل قادر به غیر فعال‌سازی آن و لغو مجوز اعطاشده می‌باشد.

"Secure Enclave"بخشی از تراشه‌های A7 و جدیدترین تراشه‌ای است که برای Touch ID استفاده می‌شود.

گوشی‌های اندروید تحت دستورالعمل‌های مشابه کار می‌کنند. آن‌ها داده‌های اثر انگشت را در قسمت امن پردازشگر اصلی به نام "Trusted Execution Environment" یا به‌طور خلاصه TEE نگه می‌دارند. TEEاز دیگر قسمت‌های پردازنده جدا می‌باشد و به‌طور مستقیم با برنامه‌های نصب‌شده ارتباط برقرار نمی‌کند.

مانند دستگاه‌های اپل، داده‌های اثر انگشت در حالت رمزگذاری شده ذخیره می‌شوند. علاوه بر این، هنگامی‌که کاربری از دستگاه استفاده نمی‌کند، باید هرگونه اثر انگشت ذخیره‌شده بر روی آن حذف شود.

در حالی‌که سایر دستگاه‌ها هنوز متکی به روش اثر انگشت هستند، اپل تکنولوژی اسکن اثرانگشت را تغییر داد و شناساگر چهره را با شناساگر اثر انگشت جایگزین کرد.

درواقع، در سال ۲۰۱۸، بسیاری از توسعه‌دهندگان گوشی‌های هوشمند قصد دارند اسکنر اثر انگشت را بر روی صفحه‌نمایش خود قرار دهند. Vivo اولین شرکتی است که چنین دستگاهی را عرضه می‌کند. گوشی Vivo دارای یک سنسور CMOS Synaptic و یک دوربین کوچک که در زیر نمایشگر قطعه می‌باشد.

هر زمان که صفحه OLED روشن می‌شود حسگر، اثر انگشت شما را نیز می‌بیند و سپس آن را با اطلاعاتی که قبلاً ذخیره‌شده مقایسه می‌کند. برای کاربران، نتیجه مشابه روش قبل است، صفحه را با انگشت خود لمس می‌کنند و گوشی آنها باز می‌شود.

۱۲-٤-۲- اسکنر چشم

محققان امنیتی، چشم را یکی از قابل اطمینان‌ترین قسمت‌های بدن برای احراز هویت بیومتریک می‌دانند، زیرا شبکیه و عنبیه در طول عمر فرد کاملاً بدون تغییر باقی می‌مانند.

- یک اسکنر شبکیه، عروق خونی پیچیده در چشم یک فرد را با استفاده از نور مادون قرمز روشن می‌کند و باعث می‌شود که قسمت بیشتری از بافت اطراف قابل‌مشاهده باشد. دقیقاً مانند اثرانگشت، دو نفر هرگز نمی‌توانند یک الگوی شبکیه مشابه به هم را داشته باشند.
- اسکنرهای عنبیه چشم به عکس یا فیلم‌های با کیفیت بالا از یک یا هر دو عنبیه چشم وابسته هستند. عنبیه چشم نیز منحصر به فرد است. با این حال ثابت شده، اسکنرهای عنبیه به‌سادگی با استفاده از یک عکس با کیفیت بالا از چهره یا چشم‌های شخص فریب می‌خورند.

۱-۲-۴-۱۲- اسکنر عنبیه چشم چگونه کار می‌کند؟

هنگامی‌که حرف از بیومتریک است، عنبیه چشم دارای چندین مزیت عمده در مقایسه با اثر انگشت است:

- شما هر بار که چیزی را لمس می‌کنید اطلاعاتی را منتشر نمی‌کنید.
- عنبیه در طول زندگی شخص عملاً بدون تغییر باقی می‌ماند. از طرف دیگر یک اثر انگشت می‌تواند کثیف، زخمی و یا مرطوب باشد.
- شما نمی‌توانید یک اثرانگشت را با دست‌های کثیف و عرق کرده استفاده کنید. ولی عنبیه چشم چنین مشکلی ندارد.
- تنها عیب اصلی اسکنر عنبیه این است که عکس‌های با کیفیت بالا از چشم یا چهره شما می‌توانند اسکنر را فریب دهند و دستگاه را باز کنند.

باوجود این محدودیت‌ها، تکنولوژی بیومتریک به‌عنوان یک ویژگی امنیتی در فرودگاه‌ها، بانک‌ها و دیگر سازمان‌های حساس استفاده می‌شود. البته، درست مثل سایر مشخصه‌های امنیتی، از تکنولوژی‌های احراز هویت چندگانه در آنها استفاده می‌شود.

نحوه عملکرد آنها چنین است، در مرحله ثبت‌نام، اسکنر با استفاده از هر نور طبیعی و همچنین نور مادون قرمز عکس عنبیه را با دقت بالا می‌گیرد؛ زیرا در غیر این صورت عنبیه چشم قابل مشاهده نیست.

پس از آنکه دستگاه مشخصات عنبیه فرد را ثبت کرد، جزئیات غیرضروری مانند مژه‌ها را حذف می‌کند، سپس اطلاعات را به داده‌های ریاضی تبدیل می‌کند و آنها را رمزگذاری می‌کند.

برای تأیید نهایی، یک اسکنر عنبیه دوباره نور مادون‌قرمز را برای شناسایی بهتر جزئیات پنهان به چشم می‌تاباند. از آنجا که یک اسکنر عنبیه نور خود را تأمین می‌کند، در شرایط تاریک نیز کار می‌کند.

۱۲-٤-۳- شناسایی متکلم

شناساگر متکلم، برعکس شناساگر صدا، می‌خواهد کسی را که صحبت می‌کند شناسایی کند و نه حرفی که گفته می‌شود.

به‌منظور شناسایی متکلم، نرم‌افزار تخصصی، کلمات شما را به بسته‌های فرکانسی تجزیه می‌کند که فورمنت نامیده می‌شوند. این بسته‌های فورمنت نیز شامل یک تن صدایی از کاربر بوده و این دو با هم، مدل صدای شما را تشکیل می‌دهند.

فورمنت را به‌عنوان "قله طیفی" طیف صدا تعریف می‌کنند. انجمن آکوستیک آمریکا یک فورمنت را چنین تعریف می‌کند: "طیف وسیعی از فرکانس‌ها که در آن حداکثر مطلق یا نسبی در طیف صدا وجود دارد".

۱-۳-۴-۱۲- فناوری تشخیص متکلم می‌تواند

- به متن بستگی داشته باشد، به این معنی که پس از شناسایی کلمات یا عبارات خاص همچنان آن را باز کند.
- مستقل از متن باشد، یعنی در این حالت سعی می‌کند صدای خود شما را تشخیص دهد و آنچه که درواقع گفته می‌شود را نادیده می‌گیرد.

برخلاف سایر روش‌های ذکر شده در اینجا، تشخیص متکلم یک مشکل دارد و آن این است که صداهای پس‌زمینه و صداهای موجود در محیط پیرامون، صدای شخص را از شکل طبیعی خارج می‌کند و تشخیص درست غیرممکن می‌شود. اما بزرگ‌ترین مسئله برای تشخیص متکلم این است که چگونه می‌توان یک نمونه صدای ضبط شده با کیفیت بالا ایجاد کرد. حتی تلفن‌های هوشمند با کیفیت پایین نیز می‌توانند صدای شخص، آهنگ صدا، تن و لهجه را با دقت کامل ضبط کنند.

این مشکل، شناساگر متکلم و تکنولوژی‌های مشابه به آن را از رسیدن به مسیر اصلی متوقف نکرده است. منظور ما سوءاستفاده از احراز هویت بیومتریک نیست، بلکه منظورمان روش‌های "کلاسیک" هکرهاست. آزمایشگاه‌های امنیتی Rhino نشان دادند که مهاجمان چگونه از طریق وای‌فای به Amazon Keyحمله می‌کنند تا دوربین‌های امنیتی تعبیه‌شده در منزل، فیلم افرادی را که وارد خانه می‌شوند، ضبط نکنند.

۱۲-٤-٤- سایر فناوری‌های بیومتریک

روش‌های بالا شناخته‌شده‌ترین و محبوب‌ترین آنها هستند، اما تنها این موارد نیستند. در این قسمت به برخی دیگر از این فن‌آوری‌ها اشاره‌شده است:

۱-۴-۴-۱۲- تشخیص چهره

به‌طورکلی، سیستم‌های تشخیص چهره از بسیاری از روش‌های احراز هویت بیومتریک استفاده می‌کنند.

روش کلاسیک آن، این است که به‌راحتی ویژگی‌های چهره خود را چشم‌ها، بینی، فاصله بین لب‌ها و از یک تصویر استخراج کنید و آنها را با سایر تصاویر مقایسه کنید تا یک همخوانی و شباهت پیدا کنید.

روش مدرن آن با تجزیه و تحلیل بافت پوست، خطوط منحصر به‌فرد، علائم زیبایی، چین و چروک و ... در چهره شما به یک فضای ریاضی تبدیل می‌شوند که بعداً با سایر تصاویر مقایسه می‌شوند.

هر دو روش را می‌توان به‌راحتی با آرایش، ماسک و یا در برخی موارد، به‌سادگی با پوشش بخشی از چهره خود فریب داد. این همان‌جایی بود که با به‌کارگیری تصاویر حرارتی و سایر تکنولوژی‌ها این بازی را قبل از رسیدن به اوج خود متوقف ساختیم که از استقبال گسترده سیستم‌هایی مانند Apple برخوردار شد.

شناساگر چهره آیفون از بیش از ۳۰ ۰۰۰ نقطه مادون‌قرمز برای تعیین مدل چهره شما استفاده می‌کند، سپس یک نقشه سه‌بعدی از ویژگی‌های چهره شما را ایجاد می‌کند. این نقشه به Enclave Secure در پردازنده فرستاده می‌شود تا با داده از پیش ذخیره شده در دستگاه مقایسه شود. اپل برای بازاریابی‌های خود گفته است که از بین یک‌میلیون فرصت برای باز کردن قفل آیفون تنها یک شانس با استفاده از شناساگر چهره وجود دارد. البته، این فقط به‌عنوان یک چالش برای کارشناسان امنیتی به نظر می‌رسد. یک محقق از ویتنام شناساگر چهره را با یک ماسک سه‌بعدی چاپ‌شده از نوار سیلیکون و کاغذ فریب داد.

۱۲-٤-٥- هندسه و شکل کف دست و انگشتان

این روش هرچند به منحصر به فردی اثر اسکن عنبیه چشم و یا چهره‌نگاری سه‌بعدی نیست، اما از آنجا که دست ما تا حدودی متفاوت از دست سایر افراد است، این روش در شرایط خاص می‌تواند، یک روش احراز هویت قابل اعتماد باشد.

اسکنر دست، شکل و هندسه، ضخامت کف دست، طول و عرض انگشتان و غیره را اندازه‌گیری می‌کند. مزایای استفاده از این نوع سیستم کم‌هزینه بودن، سهولت استفاده و محبوبیت آن است. این مورد نیز دارای چند عیب عمده است. اندازه دست در طول زمان می‌تواند متفاوت باشد. مشکلات بهداشتی ممکن است حرکات را محدود کنند. مهم‌تر از همه، یکدست به‌اندازه کافی منحصر به فرد نیست، بنابراین دقت سیستم کم است.

۱-۵-۴-۱۲- هندسه رگ‌ها

طرح رگ‌های ما کاملاً منحصر به فرد است و حتی برای دوقلوها هندسه و شکل مشابهی ندارند. درواقع طرح کلی رگ‌ها از یکدست تا دست دیگر متفاوت است. مزیت اضافه‌ای که رگ‌ها دارند این است که کپی کردن و سرقت از طریق آنها به طرز باورنکردنی دشوار است زیرا آنها تحت شرایطی کاملاً خاص قابل‌مشاهده هستند. یک اسکنر هندسی رگه‌ای، می‌تواند رگ‌ها را با نور کم مادون‌قرمز روشن کند و درنتیجه رگ‌ها روی تصویر قابل‌مشاهده باشند.

۱۲-۵- مزایا و معایب احراز هویت بیومتریک

درنهایت، همه تکنیک‌های احراز هویت بیومتریک مربوط به امنیت است. اگر آن را به عنوان یک قابلیت بدانیم رقیب اصلی آنها رمز عبورها (و یا در موارد خاص پین کدها) هستند و مقایسه بین این دو، نقاط ضعف آنها را نشان می‌دهد.

در واقع مدیران سازمان‌ها و کسب‌وکارها همواره در تلاش هستند که نقص‌های امنیتی ناشی از کلمه‌های عبور معمولی که منجر به ایجاد حفره‌هایی بین امنیت و کاربردی بودن شده‌اند را برطرف نمایند. کاربرانی که از روش‌های احراز هویت مرسوم نیز دلخور و ناراضی بودند خواستار استفاده از این فناوری امنیتی شدند. بر اساس مطالعات صورت گرفته، حدود دو سوم از افراد خواهان استفاده از روش‌های احراز هویت بیومتریک در پرداخت‌های آنلاین خود بوده‌اند.

۱۲-۵-۱- مزایا

۱-۱-۵-۱۲- سهولت استفاده

استفاده از اثر انگشت یا اسکن عنبیه چشم بسیار آسان‌تر از استفاده از یک رمز عبور است، به‌ویژه اگر رمز عبور طولانی باشد. برای گوشی هوشمند که بتواند یک اثر انگشت را شناسایی کند و به کاربر اجازه دسترسی به تلفن را بدهد، تنها یک ثانیه طول خواهد کشید. اسکنرهای اولتراسونیک به‌زودی رایج می‌شوند، زیرا تولیدکنندگان می‌توانند آن را به‌طور مستقیم در پشت صفحه‌نمایش قرار دهند، بدون اینکه هرگونه شرایط اضافه‌ای را بر روی یک گوشی قرار دهند.

از سوی دیگر، تشخیص صدا منوط به برقراری شرایطی است و صداهای پس‌زمینه می‌توانند به‌راحتی فرایند را متوقف کنند و آن را غیر عملی سازند. بر اساس آمار و نتایج مؤسسات تحقیقاتی، بیومتریک صدا حدود ۹۰ درصد از کلاهبرداری‌های صورت گرفته از طریق کانال‌های صوتی و گوشی موبایل را تشخیص می‌دهد.

فناوری احراز هویت از طرق مختلفی از جمله صدا، اثر انگشت یا تصویر سلفی انجام می‌شود که هرکدام از آنها نیز با طرح یک پرسش از کاربر و تأیید آن توسط وی برای انجام عمل مشخصی فعال می‌شود. مثلاً در احراز هویت از طریق تکنولوژی بیومتریک صدا، تماس‌گیرنده پرسش‌هایی را به صورت پی در پی مطرح می‌کند و صدای کاربر را حین اینکه به سؤالات مطرح شده پاسخ می‌دهد، با پرینت صدای اصلی کاربر در یک تماس طبیعی تطبیق می‌دهد.

۱۲-۵-۲- معایب

۱-۲-۵-۱۲- اثر انگشت کلیدی

هنگامی که برای اولین بار می‌خواهید اثر انگشت خود را ثبت کنید، دستگاه شما از چندین زاویه مختلف اثرانگشت شما را می‌خواهد. سپس این نمونه‌ها به‌عنوان داده‌های اصلی با تلاش‌های بعدی که برای باز کردن دستگاه مورداستفاده قرار می‌گیرند، مقایسه می‌شوند.

اگرچه، سنسورهای گوشی‌های هوشمند کوچک هستند، ولی اغلب به موارد جزئی از اثر انگشت دست می‌یابند. محققان کشف کرده‌اند که مجموعه‌ای متشکل از ۵ "اثر انگشت کلیدی "می‌تواند از این تطبیق‌های جزئی بهره‌برداری کند و حدود ۶۵ درصد از دستگاه‌ها را باز کند. این تعداد به‌احتمال زیاد در شرایط فعلی، کمتر است اما نرخ حقیقی آن حتی اگر ۱۰ الی ۱۵ درصد باشد بازهم زیاد است و می‌تواند میلیون‌ها دستگاه را تحت تأثیر قرار دهد.

۲-۲-۵-۱۲- تغییر مشخصات بیومتریک

اگر کسی رمز عبور شما را بدست آورد، همیشه می‌توانید گذرواژه خود را تغییر دهید، اما هیچ راهی برای تغییر عنبیه چشم، شبکیه یا اثر انگشت شما وجود ندارد. هنگامی‌که کسی نسخه‌ای از آنها را داشته باشد، به‌هیچ‌وجه نمی‌توانید امنیت بیشتری داشته باشید، به غیر از تغییر رمز عبور یا استفاده از اثر انگشتی دیگر.

در یکی از بزرگ‌ترین هک‌های اداره مدیریت منابع انسانی ایالات‌متحده، هکرها ۵.۶ میلیون اثرانگشت به دست آوردند و از طریق آنها نفوذ کردند. کارکنان و افراد وابسته، بخشی از هویتشان برای همیشه به خطر افتاد.

یک نکته مهم در امنیت بیومتریک این است که کاربر نمی‌تواند از راه دور آنها را تغییر دهد. اگر شما نتوانید به ایمیل خود دسترسی پیدا کنید، در این زمان شما می‌توانید یک بازیابی از راه دور داشته باشید تا دوباره آن را کنترل کنید. در طول فرایند، شما می‌توانید رمز عبور خود را تغییر دهید یا رمز عبور دو مرحله‌ای را اضافه کنید تا امنیت حسابتان را دو برابر کنید. ولی عملکرد بیومتریک این‌گونه نیست. جسم شما باید در نزدیکی دستگاه باشد تا مجموعه داده اولیه و امن آن را تغییر دهید.

یک دزد می‌تواند گوشی هوشمند شما را سرقت کند، یک اثر انگشت جعلی ایجاد کند و سپس از آن برای باز کردن قفل گوشی به‌صورت خودکار استفاده کند. مگر اینکه شما به سرعت از راه دور تلفن خود را قفل کرده باشید، هرچند یک دزد حرفه‌ای به‌سرعت بیت به بیت اطلاعات را بر روی دستگاه سرقت می‌کند.

۳-۲-۵-۱۲- آسیب‌پذیری در نرم‌افزار احراز هویت بیومتریک

چند سال پیش، محققان امنیتی نقاط ضعف دستگاه‌های اندروید را که به هکرها اجازه می‌داد تا اثر انگشت کاربر را استخراج کنند و از در پشتی نرم‌افزار برای ربودن پرداخت‌های با تلفن همراه یا حتی نصب نرم‌افزارهای مخرب استفاده کنند، کشف کردند. علاوه بر این، آن‌ها قادر به انجام این کار از راه دور بدون دسترسی فیزیکی به دستگاه بودند. پس از آن، کارهایی برای رفع آسیب‌پذیری‌های مربوط به نرم‌افزارهای احراز هویت انجام شد، اما همچنان شکارچیان حقیقی در حال شکار با موارد جدیدتر هستند.

۱۲-٦- روش‌های هک کردن

محققان امنیتی کلاه‌سفید بارها و بارها نشان داده‌اند که چگونه اسکنر اثر انگشت یا عنبیه چشم را فریب می‌دهند. در اینجا فقط به برخی از روش‌هایی که استفاده می‌کنند، اشاره شده است:

اصطلاح کلاه‌سفید در زبان عامیانه اینترنت به یک هکر کامپیوتری اخلاقی یا یک متخصص امنیتی کامپیوتر که متخصص در آزمایش نفوذ و سایر روش‌های تست برای حصول اطمینان از امنیت سیستم‌های اطلاعاتی سازمان است گفته می‌شود.

۱۲-٦-۱- ایجاد اثرانگشت جعلی

برای باز کردن یک گوشی هوشمند با یک اثر انگشت ایمن، هکر باید در ابتدا یک چاپ با کیفیت بالا را که شامل الگوهای خاص و کافی برای باز کردن دستگاه است آماده کند.

بعد، مهاجم اثر انگشت را برداشته، آن را روی یک ورقه پلاستیکی قرار داده و سپس مدل اثر انگشت را قالب‌گیری کند. هنگامی‌که هکری اثرانگشت جعلی شما را ایجاد می‌کند، تمام کاری که او باید انجام دهد این است که آن را در اسکنر قرار دهد، انگشت خود را برای انجام عملیات الکتریکی فشار دهد و سپس از تلفن باز شده استفاده کند.

۱۲-٦-۲- فریب اسکنر عنبیه چشم

برای فریب برخی از اسکنرهای عنبیه چشم، تمام کاری که باید انجام شود این است: گرفتن عکس با یک دوربین ارزان در حالت شب، چاپ عنبیه چشم بر روی کاغذ، سپس یک لنز مرطوب برای ایجاد شباهت به چشم انسان بر روی آن قرار می‌دهند.

۱۲-۶-۳- هک کردن سنسور بیومتریک و سرقت داده‌ها

یکی دیگر از روش‌های مؤثر در به دست آوردن داده‌های مربوط به اثر انگشت یک تلفن و باز کردن قفل آن این است که، هکرها مستقیماً قسمت ذخیره‌سازی اطلاعات تلفن را هک می‌کنند.

برای دستگاه‌هایiOS، این کار به معنی شکستن امنیت Enclave است. ازلحاظ فنی، این امکان‌پذیر است، اما از محدوده هک‌های روزمره هکرهای سایبری فراتر است. تعداد زیادی برای این نوع از هک توسط سلبریت[1] گزارش نشده است.

اگر کسی تلفن هوشمند شما را سرقت کند، قفل اثر انگشت بی‌فایده است، چراکه به راحتی نمونه چاپی را از دستگاه برمی‌دارد.

البته هیچ‌کدام از روش‌های احراز هویت از جمله بیومتریک صدا یا احراز هویت از طریق تصویری سلفی دارای ایمنی صد در صد نیستند؛ اما مزیت روش بیومتریک در مقایسه با سایر روش‌های احراز هویت این است که این راهکار بدون اینکه هیچ تعهد و مسئولیتی بر عهده مشتری بگذارد فرایند احراز هویت را پیچیده‌تر می‌کند. برای مثال، احراز هویت بیومتریک از طریق صدا، چندین ویژگی منحصر به فرد از جمله، خصوصیات فیزیکی مانند سایز و شکل کانال تنفسی و همچنین ویژگی‌های رفتاری شامل لهجه، تلفظ و حتی سرعت صحبت کردن را به کار می‌گیرد.

با توجه به اینکه فناوری بیومتریک میزان کلاهبرداری‌ها را در سازمان‌ها کاهش داده و همچنین آنها را قادر می‌سازد که زمانی را که صرف احراز هویت مشتریان خود می‌کنند را برای بیش‌فروشی و تبلیغ محصولاتشان بگذارند، بنابراین مدیران سازمان‌ها و همچنین سایر کاربران تمایل به استفاده از این روش دارند.

علاوه بر این سرمایه قابل توجهی از بسیاری از شرکت‌ها در صنایع مختلف پس از استفاده از تکنولوژی بیومتریک[2] به سازمان بازگشته است؛ بنابراین مدیران و کارشناسان بخش‌های امنیتی در استفاده و ترویج این فناوری در کسب‌وکارشان مطمئن هستند و تنها مسأله‌ای که وجود دارد این است که چه زمانی برای اجرای این فناوری در سازمان مناسب‌تراست.

[1] Cellebrite
[2] Biometric