تهدیدات سایبری متداول جهان

در سال ۲۰۲۲

آذرماه ۱۴۰۱

وزارت بهداشت، درمان و آموزش پزشکی

ستاد پدافند غیرعامل

تهدیدات سایبری متداول جهان در سال ۲۰۲۲

رخدادهای بی‌سابقه‌ای مانند همه‌گیری کووید۱۹ و نا آرامی‌های اجتماعی- سیاسی شدید، منجر به افزایش قابل توجه تعداد و شدّت جرایم سایبری در طول چندین سال اخیر شده است. احتمالاً شاهد پیچیده‌تر شدن تهدیدات امنیتی و در نتیجه گران‌تر شدن خسارات این تهدیدات، در آینده خواهیم بود. کارشناسان پیش‌بینی می‌کنند که هزینه‌های جهانی جرایم سایبری تا سال ۲۰۲۵ به ۱۰٫۵ تریلیون دلار خواهد رسید که ۱۵ درصد بیشتر از ۳ تریلیون دلار در سال ۲۰۱۵ است.

حفاظت پیشگیرانه، کلید جلوگیری از حمله امنیت سایبری است. طبق اعلام کارشناسان، مهمترین تهدیدات امنیت سایبری پیش روی جهان در سال ۲۰۲۲ موارد زیر بوده است :

۱۰ تهدید متداول جهان در حوزه امنیت سایبری در سال ۲۰۲۲

ردیف	تهدید	Threat
۱	مهندسی اجتماعی	**Social Engineering**
۲	از طریق شخص ثالث	**Third-party Exposure**
۳	اشتباهات پیکربندی	**Mistakes Configuration**
۴	بهداشت سایبری ضعیف	**Poor Cyber Hygiene**
۵	آسیب پذیری های ابری	**Vulnerabilities Cloud**
۶	آسیب پذیری های دستگاه موبایل	**Vulnerabilities Mobile Device**
۷	اینترنت اشیاء	**Internet of Things (IoT)**
۸	باج افزار جدید	**Ransomware**
۹	مدیریت ضعیف داده ها	**Poor Data Management**
۱۰	رویه های ناکافی پس از حمله	**Inadequate Post-Attack Procedures**

۱. مهندسی اجتماعی[1]

مهندسی اجتماعی یکی از خطرناک‌ترین تکنیک‌های هک است که توسط مجرمان سایبری استفاده می‌شود، عمدتاً به این دلیل که این روش، به جای آسیب‌پذیری‌های فنی بر خطای انسانی متکی است و همین امر، حملات را خطرناک‌تر می‌کند چرا که فریب دادن یک انسان بسیار آسان‌تر از نقض یک سیستم امنیتی است، واضح است که هکرها این را می‌دانند. طبق گزارشVerizon's Data Breach Investigations، ۸۵ درصد از کل نقض‌های داده از طریق تعامل انسانی است.

در سال ۲۰۲۳، احتمالاً شاهد رشد حملات مهندسی اجتماعی مانند فیشینگ و جعل هویت از طریق ایمیل خواهیم بود؛ البته با روندها، فناوری‌ها و تاکتیک‌های جدید. به عنوان مثال، حملات مربوط به ارزهای دیجیتال بین اکتبر ۲۰۲۰ و آوریل ۲۰۲۱ تقریباً ۲۰۰ درصد افزایش یافت و احتمالاً با ادامه رشد محبوبیت و قیمت بیت کوین و سایر ارزهای مبتنی بر بلاک چین، تهدیدی برجسته باقی خواهند ماند.

[1] Social Engineering

۲. از طریق شخص ثالث[۲]

مجرمان سایبری می توانند از طریق هک کردن شبکه ها با امنیت کمتر، متعلق به اشخاص ثالث که دارای دسترسی هستند به اهداف خود دست یابند و سیستم های امنیتی را دور بزنند.

یکی از نمونه‌های مهم نقض شخص ثالث در ابتدای سال ۲۰۲۱ رخ داد که هکرها اطلاعات شخصی بیش از ۲۱۴ میلیون حساب فیس‌بوک، اینستاگرام و لینکدین را فاش کردند. هکرها با نفوذ به یک پیمانکار شخص ثالث به نام Socialarks که توسط هر سه شرکت استخدام شده بود و دسترسی بالایی داشت، توانستند به داده ها دسترسی پیدا کنند.

در سال ۲۰۲۳، نقض‌های شخص ثالث به تهدیدی مبرم‌تر تبدیل خواهند شد، زیرا شرکت‌ها به طور فزاینده‌ای به پیمانکاران مستقل روی خواهند آورند.

بر اساس یک گزارش در سال ۲۰۲۱، بیش از ۵۰ درصد از کسب و کارها به دلیل تغییر رویه به دورکاری ناشی از کووید۱۹، تمایل بیشتری به استخدام افراد خوداشتغال[۳]دارند. شرکت امنیت سایبری CyberArk گزارش می‌دهد که ۹۶ درصد سازمان‌ها به اشخاص ثالث، اجازه دسترسی به سیستم‌های حیاتی را می‌دهند و یک مسیر دسترسی بالقوه و محافظت‌نشده به داده‌هایشان را برای هکرها فراهم می‌کنند. طبق آمار، ۷۵ درصد از حملات سایبری در سال ۲۰۲۰ از آسیب‌پذیری‌هایی استفاده کرده‌اند که حداقل دو سال قبل کشف شده بودند.

[2] Third-Party Exposure
[3] Freelancer

۳. اشتباهات پیکربندی[4]

حتی سیستم‌های امنیتی حرفه‌ای، حداقل یک خطا در نحوه نصب و یا راه اندازی نرم افزار دارند. در پژوهشی که توسط شرکت نرم‌افزار امنیت سایبری Rapid7 انجام شد، ۸۰ درصد از تست‌های نفوذ خارجی به علت پیکربندی نادرست قابل بهره‌برداری بودند. در مواردی که مهاجم به سیستم داخلی دسترسی داشت (یعنی تست هایی شبیه به دسترسی از طریق شخص ثالث یا نفوذ فیزیکی به یک دفتر) میزان خطاهای پیکربندی قابل بهره‌برداری به ۹۶ درصد رسید.

در سال ۲۰۲۲، تأثیر عواملی چون همه‌گیری کووید-۱۹، تحولات اجتماعی- سیاسی و استرس مالی مداوم، احتمالاً تعداد اشتباهات و بی دقتی‌های کارکنان را در محل کار افزایش می دهد و این امر فرصت‌های بیشتری را برای مجرمان سایبری ایجاد می‌کند.

بر اساس گزارشLyra Health، ۸۱ درصد از کارکنان مشکلات سلامت روان را در نتیجه همه‌گیری تجربه کرده اند و ۶۵ درصد از کارکنان اظهار داشتند که سلامت روان آنها به طور مستقیم بر عملکرد کاری آنها تأثیر گذاشته است.

مؤسسهPonemon گزارش می‌دهد، نیمی از کارشناسان فناوری اطلاعات اذعان می‌کنند در خصوص اینکه ابزارهای امنیت سایبری نصب شده واقعاً چقدر خوب کار می‌کنند آگاهی کافی ندارند، به این معنی که حداقل نیمی از کارشناسان فناوری اطلاعات در حال حاضر تست‌های داخلی، تعمیر و نگهداری منظم را انجام نمی‌دهند.

[4] Cofiguration Mistakes

۴. بهداشت سایبری ضعیف[5]

بهداشت سایبری، به عادت‌ها و شیوه‌های منظم در مورد استفاده از فناوری، مانند اجتناب از شبکه‌های WiFi محافظت‌نشده یا احراز هویت چندعاملی اشاره دارد. تحقیقات نشان می دهد نزدیک به ۶۰ درصد از سازمان ها برای مدیریت رمزهای عبور به حافظه انسانی متکی هستند و ۴۲ درصد از سازمان‌ها رمزهای عبور را با استفاده از کاغذهای یادداشت چسب‌دار مدیریت می‌کنند. بیش از نیمی (۵۴٪) از متخصصان فناوری اطلاعات برای دسترسی به حساب های شرکت نیازی به استفاده از احراز هویت دو مرحله ای ندارند و فقط ۳۷درصد از افراد از احراز هویت دو مرحله ای برای حساب های شخصی استفاده می‌کنند. کمتر از نیمی (۴۵٪) از جامعه آماری مورد بررسی می گویند که پس از نقض اطلاعات رمز عبور خود را تغییر می دهند و فقط ۳۴درصد می گویند که رمز عبور خود را به طور منظم تغییر می دهند.

با توجه به افزایش دورکاری‌ها، سیستم‌هایی با رمزهای عبور ضعیف، از شبکه‌های محافظت‌نشده خانگی قابل دسترسی هستند، رمزهای عبور روی کاغذهای یادداشت چسب‌دار راه خود را به کافی‌شاپ‌های عمومی باز کرده‌اند و کارکنان با سیستم های شخصی وارد حساب کاربری خود می‌شوند که احتمال گم شدن یا سرقت این سیستم های شخصی بسیار بیشتر است. شرکت‌ها و افرادی که شیوه‌های سایبری خود را بهبود نمی‌دهند، اکنون در معرض خطر بسیار بزرگتری نسبت به قبل هستند.

با کمال تعجب، متخصصان فناوری اطلاعات اغلب عادات بهداشت سایبری بدتری نسبت به سایرین دارند؛ ۵۰ درصد از کارکنان فناوری اطلاعات اظهار داشتند که از رمزهای عبور تکراری و مجدد در حساب‌های کاربری محل کار خود استفاده می‌کنند.

[5] Poor Cyber Hygiene

۵.آسیب‌پذیری‌های ابری[6]

ممکن است تصور شود که فضای ابری در طول زمان امن‌تر خواهد شد اما در واقع برعکس است؛ طبق گزارش IBM، آسیب‌پذیری‌های ابری در پنج سال گذشته ۱۵۰ درصد افزایش یافته است.

به گزارش گارتنر، امنیت ابری در حال حاضر به عنوان سریع ترین بازار رو به رشد درحوزه امنیت سایبر است. تحولات جدید در امنیت ابری شامل پذیرش معماری امنیت ابری "Zero Trust" است.

Zero Trust یک طراحی استراتژیک است که با حذف مفهوم اعتماد از معماری شبکه یک سازمان، برای جلوگیری از نقض موفقیت آمیز برای امنیت بیشتر داده ها اجرا می‌گردد و ریشه در اصل "هرگز اعتماد نکنید، همیشه تحقیق کنید" دارد.

سیستم‌های ZeroTrust به گونه‌ای طراحی شده‌اند که به جای اعطای دسترسی پایدار به دستگاه‌ها یا دستگاه‌های شناسایی شده در محیط شبکه، تأییدیه‌های مورد نیاز را در هر مرحله و با هر بار ورود به سیستم اجرا می‌کنند. این سبک از امنیت در سال ۲۰۲۱ محبوبیت پیدا کرد و احتمالاً در سال‌های آینده مورد پذیرش گسترده‌تری قرار خواهد گرفت.

[6] Cloud Vulnerabilities

۶. آسیب پذیری‌های دستگاه موبایل[۷]

یکی از تمایلات ناشی از همه‌گیری کووید۱۹، افزایش استفاده از تلفن‌های همراه بود. نه تنها کاربران راه دور بیشتر به تلفن‌های همراه متکی هستند، بلکه کارشناسان حوزه بهداشت نیز به منظور محدود کردن انتقال میکروب‌ها به پذیرش گسترده کیف پول‌های موبایل و فناوری پرداخت الکترونیکی تشویق کرده‌اند. با افزایش این گرایش، این طیف ازکاربران، اهداف حمله را برای مجرمان سایبری تشکیل دادند.

آسیب‌پذیری‌های تلفن‌های همراه با افزایش دورکاری‌ها، تشدید و منجر به افزایش تعداد شرکت‌ها با سیاست «دستگاه خودت را بیاور» شده است. بر اساس گزارش امنیتی Check Point Software در طول سال ۲۰۲۱، ۴۶درصد از شرکت ها با یک حادثه امنیتی مرتبط با یک برنامه مخرب تلفن همراه که توسط یک کارمند دانلود شده بود، مواجه شدند. مجرمان سایبری شروع به هدف قرار دادن دستگاه‌های تلفن همراه کرده‌اند.

[7] Mobile Device Vulnerabilities

۷. اینترنت اشیاء[8]

الگوی دورکاری ناشی از همه گیری کووید۱۹، منجرشد بیش از یک چهارم از کارمندان کارهای خود را به خانه ببرند، مکانی که ۷۰ درصد از خانواده‌ها حداقل دارای یک دستگاه هوشمند هستند؛ در نتیجه حملات به دستگاه‌های هوشمند یا «اینترنت اشیاء» افزایش یافت و بیش از ۱,۵ میلیارد نقض داده بین ژانویه و ژوئن ۲۰۲۱ رخ داد.

به طور متوسط یک دستگاه هوشمند در عرض پنج دقیقه پس از اتصال به اینترنت می تواند مورد حمله قرار می‌گیرد و کارشناسان تخمین می‌زنند که یک خانه هوشمند با طیف گسترده‌ای از دستگاه‌هایIoT ممکن است در یک هفته مورد هدف ۱۲۰۰۰ حمله هک قرار گیرد.

محققان پیش‌بینی می‌کنند که تعداد دستگاه‌های هوشمند سفارش‌داده شده بین سال‌های ۲۰۲۱ تا ۲۰۲۵ دو برابر خواهد شد و این موضوع، شبکه‌ای گسترده‌تر از نقاط دسترسی ایجاد می‌کند که می‌توانند برای نقض سیستم‌های شخصی و شرکتی مورد هدف قرار گیرند. انتظار می‌رود تعداد اتصالات اینترنت اشیاء در سال ۲۰۲۳ به ۳,۵ میلیارد برسد و کارشناسان پیش بینی می‌کنند که بیش از یک چهارم حملات سایبری علیه مشاغل تا سال ۲۰۲۵ مبتنی بر اینترنت اشیاء خواهد بود.

[8] Internet of Things

۸. باج افزار[9]

در حالی که حملات باج افزار تهدید جدیدی محسوب نمی‌شوند، مبالغ درخواستی برای دریافت باج در سال های اخیر به طور قابل توجهی سیر صعودی داشته است؛ بین سال های ۲۰۱۸ تا ۲۰۲۰ میانگین هزینه باج از ۵۰۰۰ دلار به ۲۰۰۰۰۰ دلار افزایش یافته است.

متوسط مدت زمان خرابی سیستم پس از حمله باج افزار ۲۱ روز است. در یک نظرسنجی در سال ۲۰۲۱ از ۱۲۶۳ متخصص امنیت سایبری، ۶۶ درصد اظهار داشتند که شرکت های آنها در اثرحمله باج افزار، هزینه هنگفتی را از دست داده است. از هر سه یک نفر بیان داشتند که شرکت آنها با اخراج یا استعفاء، مقام ارشد خود را از دست داده است و ۲۹ درصد اظهارداشتند که شرکت آنها مجبور به حذف مشاغل به دنبال حمله باج افزار شده است.

به مرور زمان باج افزارها برای استفاده‌ی هکرها پیچیده تر، دردسترس‌تر و راحت‌تر شده‌اند. در واقع، مجرمان سایبری اکنون می‌توانند به عنوان فراهم کنندگان باج افزار به عنوان یک سرویس فعالیت کنند، که به کاربران اجازه می‌دهد ابزارهای باج‌افزاری از پیش توسعه‌یافته را برای اجرای حملات در ازای درصدی از تمام پرداخت‌های موفق باج‌گیری، مستقر کنند. ظهورپدیده «باج افزار به عنوان سرویس»[10] به این معنی است که حملات باج‌افزار اکنون به‌طور قابل‌توجهی برای مجرمان سایبری مقرون‌به‌صرفه و این دست حملات همچنان رو به افزایش است.

[9] Ransomware
[10] RaaS: Ransomware-as-a-Service

۹. مدیریت ضعیف داده ها[1]

مدیریت داده، چیزی بیش از مرتب نگه داشتن سیستم های ذخیره‌سازی و سازمانی است. داده های ایجاد شده توسط کاربران هر چهار سال دو برابر می شود، اما بیش از نیمی از این داده های جدید هرگز استفاده یا تجزیه و تحلیل نمی شوند. انبوهی از داده های مازاد منجر به ایجاد سردرگمی می شوند که داده ها را در برابر حملات سایبری آسیب پذیر می کند.

نقض‌های ناشی از اشتباهات مدیریت داده‌ها می‌تواند به اندازه حملات امنیت سایبری پرهزینه باشد.

ایتنا، شرکت خدمات درمانی امریکایی، پس از ارسال اطلاعات حسّاس بهداشتی در پاکتی اشتباه، به پرداخت ۱۷ میلیون دلار در سال ۲۰۱۸محکوم شد.

به دلیل انفجار داده‌ها که در دهه گذشته اتفاق افتاده است، کارشناسان پیش‌بینی می‌کنند که سال ۲۰۲۲ تغییری فزاینده از «داده‌های بزرگ[2]» به سمت «داده‌های درست[3]» یا تأکید بر ذخیره داده‌های موردنیاز را به همراه خواهد داشت.

برای مرتب‌سازی و جدایی داده‌های درست از داده‌های غیرضروری، به طور فزاینده‌ای بر اتوماسیون تأکید می گردد که این امر نیز خطرات خاص خود را در پی دارد، از آنجا که پردازش داده ها متکی به هوش مصنوعی است و قوانین و تنظیماتی که هوش مصنوعی باید از آنها پیروی کند، توسط انسان ایجاد می شود، این حوزه نیز مستعد خطای انسانی است.

[1] Poor Data Management [1]
[1] Big Data [2]
[1] Right Data [3]

۱۰. رویه های ناکافی پس از حمله[1]

حفره‌های امنیتی باید بلافاصله پس از حمله امنیت سایبری اصلاح شوند. دریک نظرسنجی در سال ۲۰۲۱ از ۱۲۶۳ شرکتی که هدف نقض امنیت سایبری قرار گرفته بودند، ۸۰ درصد از قربانیانی که پرداخت باج را فراهم کردند، اظهار داشتند که بلافاصله پس از آن حمله دیگری را تجربه کرده‌اند.

در واقع، ۶۰ درصد از حملات سایبری در صورت اِعمال وصله‌های موجود، قابل پیشگیری بودند و ۳۹ درصد از سازمان‌ها اعلام داشتند که قبل از وقوع حمله سایبری از آسیب‌پذیری خود آگاه بودند.

سال آینده شاهد پس لرزه‌های حملات امنیت سایبری سال ۲۰۲۱ خواهیم بود که به دلیل کووید۱۹ به طور تصاعدی افزایش یافت. توانایی مدیریت وصله، توسط سازمان‌هایی که در سال ۲۰۲۱ هدف قرار گرفتند، تعیین می‌کند که آیا در سال آینده قربانی حمله دیگری شوند یا خیر.

یکی از راه حل‌های رایج، انتخاب مدلی مشترک برای نرم افزار مدیریت وصله است. محصولات «وصله به عنوان سرویس»[2]روزرسانی‌ها و وصله‌های مداوم را ارائه و سرعت و کارایی وصله را افزایش می‌دهند. همچنین وصله‌زنی خودکار احتمال آسیب‌پذیری‌های وصله با خطای انسانی را کاهش می‌دهد.

[1] Inadequate Post-Attack Procedures

[2] Patching-as-a-Service