شرکت آب منطقه‌ای گلستان

نشریه داخلی شرکت آب منطقه‌ای گلستان/ شماره اول / فروردین ماه ۱۴۰۴

امنیت دیجیتال را از کجا شروع کنیم؟

DIGITAL SECURITY

KEVIN MITNICK

شرکت ها میلیون ها دلار را برای فایروال‌ها، رمزگذاری و دستگاه‌های دسترسی ایمن خرج می‌کنند و این پول هدر می‌رود. هیچ یک از این اقدامات به ضعیف‌ترین حلقه در زنجیره امنیتی یعنی منابع انسانی، نمی‌پردازد.

نشریه داخلی شرکت آب منطقه‌ای گلستان

شماره اول — فروردین ماه ۱۴۰۴

فهرست

دکتر امیرحسین رحیمیان

چرا امنیت دیجیتال مهم‌تر از همیشه است؟

در دنیای امروز، امنیت دیجیتال دیگر یک انتخاب نیست، بلکه ضرورتی است که زندگی شخصی، شغلی و اجتماعی ما را به‌طور مستقیم تحت تأثیر قرار می‌دهد. از زمانی که انسان‌ها شروع به دیجیتالی کردن اطلاعات خود کردند، چالش حفاظت از این اطلاعات نیز پدید آمد. با این حال، با گسترش روزافزون اینترنت، هوش مصنوعی، اینترنت اشیاء (IoT) و انتقال بیشتر فعالیت‌ها به بسترهای آنلاین، اهمیت امنیت دیجیتال بیش از هر زمان دیگری به چشم می‌آید. ما در جهانی زندگی می‌کنیم که تقریباً تمام فعالیت‌های روزمره ما به نوعی به اینترنت و فناوری متصل است. خرید، بانکداری، آموزش، سلامت، ارتباطات اجتماعی و حتی سرگرمی، همه به بسترهای دیجیتال وابسته شده‌اند. این اتصال گسترده به‌معنای آن است که هرگونه ضعف در امنیت اطلاعات می‌تواند پیامدهای جدی و جبران‌ناپذیری برای افراد و سازمان‌ها به همراه داشته باشد. در این قسمت، دلایل اهمیت روزافزون امنیت دیجیتال را از جنبه‌های مختلف بررسی می‌کنیم.

01 رشد حملات سایبری

آمارهای جهانی نشان می‌دهند که حملات سایبری در سال‌های اخیر به‌طور فزاینده‌ای افزایش یافته‌اند. باج‌افزارها، فیشینگ، مهندسی اجتماعی، حملات مرد میانی (MITM)، و نفوذ به شبکه‌های سازمانی تنها بخشی از تهدیداتی هستند که روزانه میلیون‌ها کاربر با آن‌ها روبرو می‌شوند. هکرها امروز فقط به دنبال سرقت اطلاعات نیستند؛ آن‌ها اطلاعات را گروگان می‌گیرند، تغییر می‌دهند یا برای اهداف سیاسی و اقتصادی از آن سوءاستفاده می‌کنند.

02 دیجیتالی شدن زندگی شخصی

اطلاعاتی که ما به صورت روزمره در فضای دیجیتال ثبت می‌کنیم، از عکس‌های خانوادگی گرفته تا اطلاعات موقعیت مکانی، سلیقه‌های خرید، علایق، پیام‌های شخصی و... همه بخش‌هایی از هویت ما در فضای مجازی را تشکیل می‌دهند. هرچه اطلاعات بیشتری از ما در فضای دیجیتال وجود داشته باشد، مسئولیت حفاظت از آن نیز بیشتر می‌شود. نشت این اطلاعات می‌تواند باعث سرقت هویت، آزار سایبری، و حتی تهدیدات فیزیکی شود.

03 گسترش دورکاری و کار از راه دور

با همه‌گیری ویروس کرونا، میلیون‌ها نفر در سراسر جهان به کار از راه دور روی آوردند. این تغییر

سبک کاری، شکاف‌های امنیتی جدیدی در زیرساخت‌ها ایجاد کرد. اتصال کارکنان از طریق شبکه‌های خانگی ناامن، استفاده از دستگاه‌های شخصی برای دسترسی به داده‌های سازمانی، و نبود نظارت فنی مناسب، خطر نفوذ به اطلاعات حساس را افزایش داد.

04

اینترنت اشیاء (IoT) و تهدیدات ناشناخته

دستگاه‌هایی مانند تلویزیون‌های هوشمند، دوربین‌های نظارتی، یخچال‌ها و حتی چراغ‌های خانه، همگی امروز به اینترنت متصل هستند. اما بسیاری از این دستگاه‌ها از استانداردهای امنیتی بالایی برخوردار نیستند. یک مهاجم می‌تواند از طریق آسیب‌پذیری در یک دوربین خانگی به کل شبکه شما نفوذ کند. در نتیجه، امنیت فقط محدود به گوشی و لپ‌تاپ نیست؛ همه چیز باید امن باشد.

05

حملات به زیرساخت‌های حیاتی

در سال‌های اخیر، شاهد حملات سایبری به زیرساخت‌های حیاتی مانند نیروگاه‌ها، بیمارستان‌ها، سامانه‌های حمل و نقل و سیستم‌های بانکی بوده‌ایم. این حملات نه‌تنها تهدیدی برای امنیت اطلاعات هستند، بلکه امنیت فیزیکی و حتی جان انسان‌ها را نیز تهدید می‌کنند.

06

قوانین و مسئولیت‌های حقوقی

کشورها قوانین سخت‌گیرانه‌تری در مورد حفاظت از داده‌ها وضع کرده‌اند. برای مثال، مقررات GDPR در اتحادیه اروپا شرکت‌ها را موظف به حفاظت دقیق از اطلاعات کاربران می‌کند. سازمان‌هایی که نتوانند امنیت دیجیتال مناسبی فراهم کنند، با جریمه‌های سنگین و آسیب به اعتبار خود روبرو خواهند شد.

07

هوش مصنوعی و تهدیدات نوظهور

در حالی که هوش مصنوعی فرصت‌های زیادی را در حوزه امنیت فراهم کرده، اما تهدیدات نوینی نیز با خود آورده است. Deepfake، تحلیل رفتاری اتوماتیک، جعل چت‌های صوتی و تصویری، و تولید خودکار بدافزارها از جمله خطرات جدیدی هستند که ناشی از سوءاستفاده از فناوری‌های نوین هستند.

08

اعتماد عمومی و اعتبار برند

برای سازمان‌ها، امنیت دیجیتال تنها یک الزام فنی نیست، بلکه یک فاکتور کلیدی در اعتمادسازی با مشتریان است. در دنیایی که رقبا زیادند، از دست رفتن اعتماد کاربران به‌دلیل نشت اطلاعات یا هک شدن سامانه‌ها، می‌تواند آسیب جبران‌ناپذیری به برند وارد کند.

09

نقش آموزش و فرهنگ‌سازی

بسیاری از نفوذهای سایبری نه از طریق نقص فنی، بلکه از طریق خطاهای انسانی صورت می‌گیرد. کلیک روی لینک‌های مشکوک، باز کردن فایل‌های ناشناس، استفاده از رمزهای ضعیف، همه رفتارهایی هستند که می‌توانند راه نفوذ مهاجمان را باز کنند. به همین دلیل، آگاهی‌رسانی و آموزش کاربران در زمینه امنیت دیجیتال، به‌اندازه ابزارهای فنی اهمیت دارد.

10

آینده‌ای وابسته‌تر به فناوری

با ظهور فناوری‌هایی مثل متاورس، بلاک‌چین، رایانش کوانتومی، و گسترش واقعیت مجازی، وابستگی بشر به فضای دیجیتال حتی بیشتر خواهد شد. اگر امنیت دیجیتال در کانون توجه قرار نگیرد، آینده‌ای که با آن روبرو می‌شویم نه‌تنها هوشمندتر، بلکه خطرناک‌تر نیز خواهد بود.

با ذکر نکات بالا نتیجه می‌گیریم که امنیت دیجیتال امروز فقط یک موضوع تخصصی نیست؛ بخشی جدایی‌ناپذیر از زندگی ماست. برای حفظ حریم خصوصی، محافظت از دارایی‌ها، ایجاد اعتماد اجتماعی و سازمانی، و آماده‌سازی برای آینده‌ای فناورانه، باید امنیت دیجیتال را جدی بگیریم. این مسیر با آموزش، سرمایه‌گذاری، و تغییر نگاه ما به داده و فناوری آغاز می‌شود. اگر امنیت نداشته باشیم، هوشمندی دیجیتال فقط یک توهم خطرناک خواهد بود.

امنیت دیجیتال برای همه

چرا باید نگران باشیم؟

امنیت دیجیتال سال‌ها به‌عنوان یک دغدغه تخصصی در میان کارشناسان فناوری اطلاعات شناخته می‌شد. اما واقعیت این است که با گسترش فناوری و اینترنت در زندگی روزمره، همه ما – فارغ از موقعیت شغلی یا میزان آشنایی با تکنولوژی – به نوعی با امنیت دیجیتال درگیر شده‌ایم. امروز حتی فردی که تنها یک تلفن هوشمند دارد و از شبکه‌های اجتماعی استفاده می‌کند نیز در معرض تهدیدات سایبری قرار دارد. این مقاله به بررسی تهدیدات واقعی برای کاربران عادی و دلایل نگرانی درباره امنیت دیجیتال می‌پردازد.

هر کاربر یک هدف بالقوه است

برخلاف تصور عمومی که فقط سازمان‌ها یا افراد معروف هدف حملات سایبری هستند، کاربران عادی همواره در معرض خطرند. چرا؟ چون ساده‌تر هدف قرار می‌گیرند. رمز عبور ضعیف، کلیک روی لینک‌های جعلی، استفاده از وای‌فای عمومی یا نداشتن آنتی‌ویروس کافی است تا هکرها به اطلاعات شخصی شما دسترسی پیدا کنند. این حملات می‌توانند شامل سرقت هویت، خالی شدن حساب بانکی یا سوءاستفاده از عکس‌ها و اطلاعات شخصی باشد.

تهدیدات روزمره پنهان‌اند

بسیاری از تهدیدات امنیتی در ظاهر بسیار بی‌ضررند. مثلاً یک QR Code روی دیوار فروشگاه، یک پیام واتساپی با لینک هدیه، یا یک تماس از کسی که ادعا می‌کند از طرف بانک زنگ زده. این‌ها همگی روش‌های رایجی هستند که مهاجمان از آن‌ها برای فریب کاربران استفاده می‌کنند. تهدیدات امروز الزاماً پیچیده و فنی نیستند؛ بلکه اغلب از طریق خطاهای انسانی رخ می‌دهند.

اطلاعات شخصی، طلاهای دیجیتالی

کاربران عادی ممکن است تصور کنند «من که چیز مهمی ندارم»، اما واقعیت این است که اطلاعات روزمره شما – از ایمیل و شماره تلفن گرفته تا موقعیت مکانی و رفتارهای آنلاین – برای بسیاری از کسب‌وکارها و البته مهاجمان سایبری ارزشمند است. اطلاعات شما فروخته می‌شود، تحلیل می‌شود، و می‌تواند برای فریب شما یا دیگران مورد استفاده قرار بگیرد.

شبکه‌های اجتماعی و فریب‌های جدید

با رشد استفاده از اینستاگرام، واتساپ، تلگرام و دیگر پلتفرم‌های اجتماعی، بستری جدید برای حملات مهندسی اجتماعی ایجاد شده است. پیام‌های فیک با وعده برنده شدن، دعوت به کانال‌های آلوده، یا حتی اکانت‌هایی که خود را به‌جای آشنایان جا می‌زنند، همه بخشی از تهدیداتی هستند که کاربران عادی را هدف می‌گیرند. کافی است یک پیام را باز کنید یا به یک درخواست پاسخ دهید تا راه نفوذ باز شود.

DIGITAL SECURITY

امنیت دیجیتال دیگر محدود به مدیران IT یا هکرهای حرفه‌ای نیست. این موضوع مستقیماً به هر فردی که گوشی، لپ‌تاپ یا اینترنت دارد مربوط می‌شود. کاربران عادی، اگر آگاه نباشند، می‌توانند هدف حملات ساده اما مؤثر قرار بگیرند. آموزش، احتیاط، و استفاده از ابزارهای مناسب می‌تواند از بسیاری از این تهدیدات جلوگیری کند. فضای دیجیتال به همان اندازه که فرصت‌آفرین است، خطرناک هم هست؛ پس امنیت را باید جدی گرفت – برای همه.

کودکان و سالمندان، قربانیان خاموش

کاربران کم‌تجربه مثل کودکان یا افراد مسن به‌راحتی قربانی حملات سایبری می‌شوند. کودک ممکن است روی لینک‌های مشکوک در بازی‌های موبایلی کلیک کند یا اطلاعات کارت بانکی والدین را وارد کند. سالمندان نیز ممکن است فریب تماس‌های فیک از مراکز دولتی یا بانک‌ها را بخورند. بدون آموزش و مراقبت، این دو گروه بسیار آسیب‌پذیر هستند.

تجهیزات خانگی هوشمند = دروازه‌های بی‌دفاع

تلویزیون‌های هوشمند، دوربین‌های امنیتی، مودم‌ها و دیگر ابزارهای متصل به اینترنت اگر به‌درستی ایمن‌سازی نشده باشند، می‌توانند به دروازه‌ای برای نفوذ مهاجمان تبدیل شوند. بسیاری از کاربران خانگی بدون تغییر رمز پیش‌فرض از این دستگاه‌ها استفاده می‌کنند، و این ساده‌ترین راه برای نفوذ است.

حملات فیشینگ: یک کلیک تا فاجعه

فیشینگ یکی از رایج‌ترین و خطرناک‌ترین حملات سایبری برای کاربران عادی است. در این روش، مهاجم وانمود می‌کند که یک نهاد قانونی (مثلاً بانک، شرکت پست یا حتی گوگل) است و کاربر را به وارد کردن اطلاعات حساس تشویق می‌کند. این حملات گاه آن‌قدر حرفه‌ای هستند که حتی کاربران با تجربه را هم فریب می‌دهند.

خریدهای اینترنتی و درگاه‌های تقلبی

کاربران زیادی برای خرید آنلاین از سایت‌هایی استفاده می‌کنند که از نظر امنیتی معتبر نیستند. برخی سایت‌ها دارای درگاه‌های پرداخت جعلی‌اند که اطلاعات کارت بانکی شما را ذخیره می‌کنند. نبود https در آدرس سایت، ظاهر ضعیف یا دامنه مشکوک می‌تواند نشانه‌هایی از جعلی بودن باشد که بسیاری از کاربران متوجه آن نمی‌شوند.

اعتماد بیش از حد به نرم‌افزارهای رایگان

نرم‌افزارهای رایگان یا کرک‌شده ممکن است حاوی بدافزار، جاسوس‌افزار یا درهای پشتی (Backdoor) باشند. بسیاری از کاربران عادی برای صرفه‌جویی در هزینه‌ها از این نرم‌افزارها استفاده می‌کنند، در حالی که ممکن است سیستم‌شان را به‌طور کامل در معرض نفوذ قرار دهند.

ضرورت آموزش و فرهنگ‌سازی

در نهایت، مهم‌ترین گام برای ایمن بودن در فضای دیجیتال، یادگیری مداوم و به‌روز ماندن است. تهدیدات سایبری همیشه در حال تغییرند، و آنچه دیروز امن بود، ممکن است امروز یک نقطه ضعف باشد. بنابراین کاربران عادی باید به‌طور منظم اطلاعات خود را درباره امنیت دیجیتال به‌روزرسانی کنند.

PASSWORD

چگونه رمز عبور قوی و مدیریت‌شده داشته باشیم؟

رمز عبور، دروازه ورود ما به دنیای دیجیتال است. هر حساب کاربری – از ایمیل گرفته تا حساب بانکی، شبکه‌های اجتماعی و حتی سرویس‌های اداری – وابسته به رمز عبور است. با وجود اهمیت بالای این موضوع، همچنان بسیاری از کاربران از رمزهای ساده، تکراری یا قابل حدس استفاده می‌کنند. در این قسمت، به‌صورت مرحله‌به‌مرحله یاد می‌گیریم که چگونه یک رمز عبور قوی بسازیم، چگونه آن را ایمن نگه‌داریم و چطور از ابزارهای مدیریت رمز عبور استفاده کنیم.

چرا رمز عبور اهمیت دارد؟

رمز عبور تنها چیزی است که بین شما و مهاجمان سایبری با نیت بد قرار دارد. اگر یک مهاجم بتواند به رمز عبور شما دست پیدا کند، می‌تواند به اطلاعات شخصی، ارتباطات کاری، اطلاعات بانکی و حتی هویت دیجیتال‌تان دسترسی پیدا کند که می‌تواند منجر به بروز فاجعه شود. بر اساس گزارش‌ها، بیش از ۸۰٪ حملات سایبری موفق به دلیل ضعف در رمز عبور رخ می‌دهد.

ویژگی‌های یک رمز عبور قوی

رمز عبور قوی باید دارای ویژگی‌های زیر باشد:

- حداقل ۱۲ کاراکتر داشته باشد
- ترکیبی از حروف بزرگ و کوچک، اعداد و نمادها باشد
- غیرقابل حدس باشد (مثل birthdate، اسم فرزند، یا ۱۲۳٤٥٦ نباشد)
- در هیچ جای دیگری استفاده نشده باشد (یکتا باشد)

مثال خوب: d#bLq۹@۷۲!Xf

مثال بد: password۱۲۳ یا reza۱۹۹۰

اشتباهات رایج کاربران در انتخاب رمز عبور

- استفاده از رمزهای رایج مانند ۱۲۳٤٥٦ یا qwerty
- استفاده از یک رمز برای چند حساب مختلف
- استفاده از اطلاعات شخصی قابل حدس (تاریخ تولد، اسم فرزند، شماره موبایل)
- نوشتن رمز عبور روی کاغذ یا در فایل‌های متنی بدون رمزگذاری

چگونه رمز عبورهای خود را مدیریت کنیم؟

مدیریت ده‌ها یا حتی صدها رمز عبور مختلف می‌تواند بسیار دشوار باشد. برای همین توصیه می‌شود از مدیر رمز عبور (Password Manager) استفاده کنید. این ابزارها به شما امکان می‌دهند:

- رمزهای قوی بسازید
- رمزها را به‌شکل رمزگذاری‌شده ذخیره کنید
- تنها با یک رمز اصلی (Master Password) به همه رمزها دسترسی داشته باشید

معرفی بهترین ابزارهای مدیریت رمز عبور

در ادامه چند ابزار معتبر و محبوب در این زمینه معرفی می‌شود:

الف) Bitwarden

- رایگان و متن‌باز
- نسخه دسکتاپ، موبایل و افزونه مرورگر
- پشتیبانی از ذخیره رمز، یادداشت امن، همگام‌سازی بین دستگاه‌ها

ب) ۱Password

- رابط کاربری ساده و زیبا
- امکان اشتراک‌گذاری رمزها با تیم یا خانواده
- دارای بخش «Watchtower» برای بررسی نشت رمزها

ج) KeePass

- رایگان و آفلاین
- نیاز به کار بیشتر برای استفاده پیشرفته، اما بسیار امن و قابل شخصی‌سازی

رمز عبور اصلی (Master Password) چیست؟

وقتی از ابزارهای مدیریت رمز استفاده می‌کنید، فقط باید یک رمز عبور اصلی قوی و به‌یادماندنی داشته باشید. پیشنهاد می‌شود:

- طولانی باشد (بیش از ۱٤ کاراکتر)
- ترکیبی از چند واژه نامرتبط (مثلا: tree-Cinema!Rocket۹)
- روی کاغذ نوشته نشود و فقط حفظ شود

فعال‌سازی احراز هویت دومرحله‌ای (۲FA)

حتی اگر رمز قوی داشته باشید، همیشه احتمال نشت اطلاعات وجود دارد. برای امنیت بیشتر، حتماً از احراز هویت دومرحله‌ای (Two-Factor Authentication) استفاده کنید. این کار باعث می‌شود حتی اگر کسی رمز شما را بداند، بدون کد ارسال‌شده به موبایل یا اپلیکیشن احراز هویت، نتواند وارد شود.

استفاده امن از مدیر رمز عبور

- نرم‌افزار را از سایت رسمی یا فروشگاه‌های معتبر دانلود کنید
- حتماً رمز اصلی قوی و منحصربه‌فرد انتخاب کنید
- از نسخه پشتیبان (Backup) رمزها در مکان امن نگهداری کنید
- از قابلیت لاگ‌اوت خودکار استفاده کنید

تغییر دوره‌ای رمزها

توصیه می‌شود رمز عبور حساب‌های مهم (مثل ایمیل اصلی یا حساب بانکی) را هر ٦ ماه یک‌بار تغییر دهید. البته اگر از مدیر رمز عبور استفاده می‌کنید، این کار ساده‌تر خواهد بود.

نکات نهایی

- هرگز رمزها را از طریق ایمیل یا پیام‌رسان برای دیگران ارسال نکنید
- از مرورگرها برای ذخیره رمز استفاده نکنید (امنیت آن‌ها پایین‌تر است)
- مراقب حملات فیشینگ باشید: هیچ سرویسی از شما نمی‌خواهد رمزتان را دوباره وارد کنید مگر از مسیر رسمی

امنیت دیجیتال با رمز عبور شروع می‌شود. انتخاب رمز قوی، استفاده از ابزارهای امن برای مدیریت آن، و رعایت اصول امنیتی، می‌تواند تا حد زیادی از تهدیدات سایبری جلوگیری کند. این کار نه‌تنها از اطلاعات شخصی شما محافظت می‌کند، بلکه به امنیت کلی فضای دیجیتال کمک می‌کند. همین امروز شروع کنید و رمزهای خود را بازبینی کنید!

CASE STUDY

••• مطالعه موردی

چگونه یک شرکت بزرگ با یک ایمیل فیشینگ هک شد؟

ماجرایی که می‌خواهید بخوانید، ساختگی نیست؛ بلکه الهام‌گرفته از حملاتی است که واقعاً در جهان رخ داده‌اند. داستان یک شرکت بزرگ مالی با صدها کارمند، هزاران مشتری، و اطلاعات محرمانه مالی. اما آن‌چه باعث شد این غول سازمانی قربانی یک نفوذ سایبری شود، نه یک بدافزار پیچیده یا هک سطح بالا، بلکه یک ایمیل ساده فیشینگ بود که به دست یکی از کارمندان رسید.

صبح روز دوشـنبه، مریم – کارمند منابع انسانی شرکت – طبق معمول پشـت میز کارش نشسـت. قهوه‌اش را برداشـت، لپ‌تاپ را روشـن کرد و شروع به بررسـی ایمیل‌های دریافتی کرد. یکـی از ایمیل‌ها با عنوان «به‌روزرسـانی فوری اطلاعات بانکی – مهلت تا سـاعت ۱۲» نظرش را جلب کرد. فرسـتنده ایمیل ظاهراً مربوط به سیستم مدیریت حقوق و دستمزد بود:

salary-updates@pay-hrsystem.com

آدرس و ظاهر ایمیل کاملاً حرفه‌ای بود؛ از لوگوی سـازمان HR گرفته تا قالب اسـتاندارد ایمیل و حتی امضای رسمی با نام مدیر منابع انسـانی. در متن ایمیـل آمده بود که به‌دلیل تغییر در سیاست‌های بانکی، لازم است تمامی کارکنان اطلاعات حساب بانکی خود را به‌روزرسـانی کنند وگرنه ممکن اسـت پرداخت حقوق این ماه با تأخیر انجام شود. لینکی نیز در ایمیل درج شده بود با عنوان «ورود به پروفایل حقوقی».

مریم، با عجله و بـدون دقت کافی، روی لینک کلیک کرد. صفحه‌ای باز شـد که بسـیار شبیه سـامانه داخلی منابع انسانی شرکت بود. فرم ورود شامل دو فیلد برای ایمیل سازمانی و رمز عبور بود. مریم اطلاعاتش را وارد کرد. صفحه بارگذاری شد و پیامی نمایشـی نشان داد: «اطلاعات شما با موفقیت ثبت شد. از همکاری شما سپاسگزاریم.»

اما این تنهـا ظاهر ماجرا بود. آن لینـک درواقع به دامنه‌ای جعلی هدایت می‌کرد: pay-hrsystem.com که شـب قبل توسط مهاجم ثبت شده بود. از نظر فنی، صفحه لاگین چیزی جز یک فرم سـاده HTML نبود که اطلاعات واردشده را مستقیماً به سـرور مهاجم ارسال می‌کرد. این یعنی مریم، ناخواسته، کلید ورود به شبکه داخلی شرکت را به دست مهاجم داده بود.

با دسترسـی به ایمیل سـازمانی مریم، مهاجم توانست وارد اینباکس، فولدرهای ذخیره‌شـده، لیسـت مخاطبیـن داخلی و حتی تقویم کاری او شـود. در ادامه، با استفاده از همان حساب کاربـری، چند ایمیـل دیگر برای کارمندان بخش مالی ارسـال شـد. این‌بار محتوای ایمیل شامل «لیسـت به‌روزرسانی حقوق کارکنان» به همراه فایلی ضمیمه و لینکی مشابه بود.

یکـی از کارمندان مالی به‌نام علیرضا، پس از دریافت ایمیل، آن را باز کرد. چون فرسـتنده، ایمیل واقعی مریم بود و محتوای ایمیل کاملاً حرفه‌ای به‌نظر می‌رسید، او هم بدون شک، لینک را باز کـرد و اطلاعات ورود خود را وارد کرد. حالا مهاجم به دو واحد کلیدی دسترسی داشت: منابع انسانی و مالی.

دسترسـی مهاجم به ایمیل‌های داخلی باعث شد او با نحوه نگارش، ساختار داخلی مکاتبات، نام مدیران و نوع فعالیت‌های مالی کاملاً آشـنا شود. در مرحله بعد، او اقدام به بارگذاری یک بدافزار سبک با ظاهر یک فایل اکسل کرد که به یکی از ایمیل‌ها ضمیمه شـده بود. پس از باز شـدن فایل توسـط کارمند سوم، بدافزار اجرا شـد و در پس‌زمینه شروع به جمع‌آوری اطلاعات کرد: از فولدرهای اشـتراکی تا نام سـرورها، لیست کاربران، و سطح دسترسی‌ها.

این نفوذ پنهان تا دو روز ادامه داشت. در این مدت، مهاجم موفق شد دسترسی به چند فولدر حساس را پیدا کند، فایل‌های مالـی رمزگذاری‌نشـده را دانلـود کند و حتی یک اسـکریپت آماده‌سـازی باج‌افـزار روی یکی از سـرورها آپلـود کند. این باج‌افزار هنوز فعال نشده بود، اما قرار بود در یک زمان مشخص فعال شود و کل داده‌های سازمان را قفل کند.

شـک تیم IT زمانی برانگیخته شـد کـه در لاگ ورود به سیسـتم‌ها، فعالیت‌هایی از یک IP خارجی غیرمعمول مشاهده شد. پس از تحلیل دقیق‌تر، مشخص شد که دو کاربر در ساعات غیـراداری و از موقعیـت جغرافیایی متفاوت به سیسـتم وارد شده‌اند. بررسی‌های فوری امنیتی آغاز شد.

تیم امنیت اطلاعات سازمان بلافاصله دست به ایزوله‌سازی شبکه زد. دسترسی کاربران مشکوک قطع شد. رمز عبورهای عمومی تغییر کرد. سیستم‌ها اسکن شدند و سرورهایی که احتمال آلودگی داشتند، از شبکه جدا شدند. در همین زمان، ارتباط با مشتریان برقرار شد و اطلاع‌رسانی درباره احتمال نشت اطلاعات صورت گرفت.

برآورد خسارت پس از حمله:

- اطلاعات بانکی بیش از ۱۲۰ نفر از کارکنان لو رفته بود.
- فایل‌های مالی داخلی شرکت و چند قرارداد حساس درز کرده بودند.
- مهاجم به داده‌هایی از مشتریان نیز دست یافته بود.
- شرکت به‌دلیل ضعف امنیتی با جریمه‌های قانونی مواجه شد.
- برای بازیابی امنیت، شرکت مجبور شد با یک تیم خارجی امنیت سایبری قرارداد چندماهه ببندد.

در تحلیل فنی این حمله، نکاتی کلیدی مشخص شد:

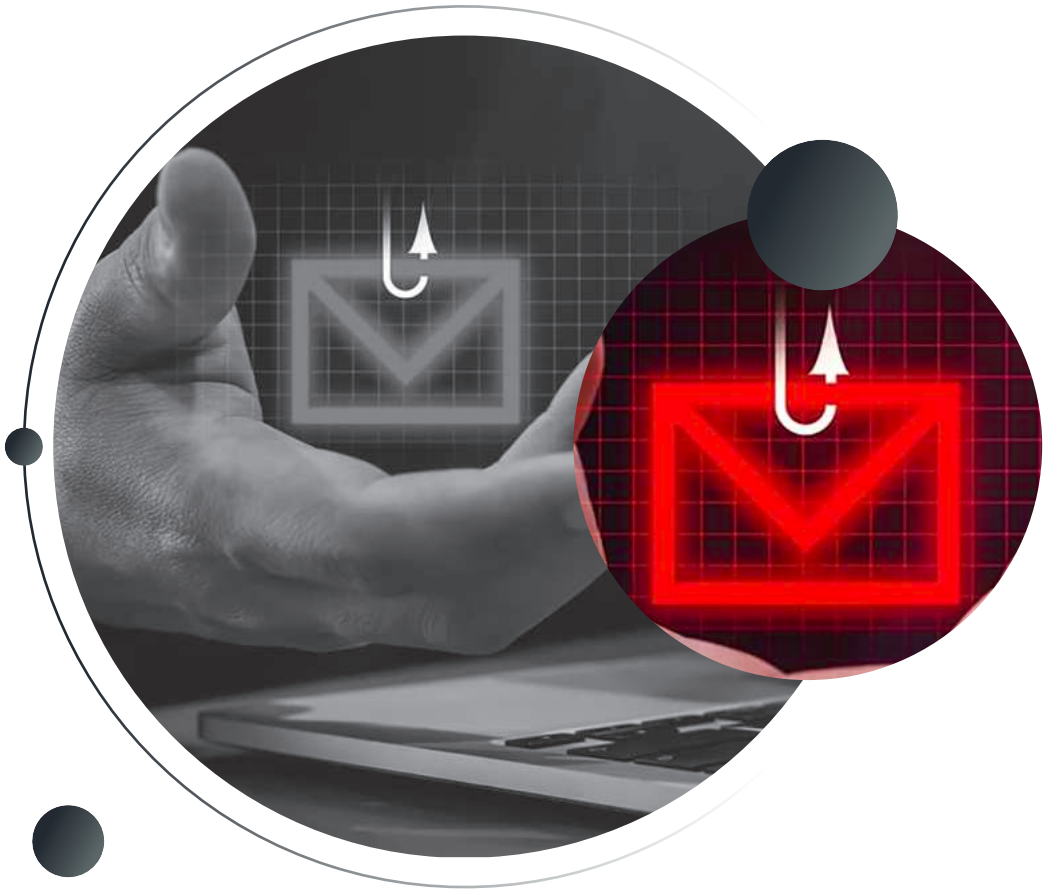
- دامنه جعلی به‌نحوی طراحی شده بود که تفاوت آن با دامنه اصلی فقط در یک خط تیره بود.
- مهاجم از HTTPS و گواهی SSL استفاده کرده بود، بنابراین صفحه فیشینگ قفل سبز داشت.
- ایمیل‌های ارسالی بسیار حرفه‌ای و بر اساس ساختار داخلی شرکت تنظیم شده بودند.
- ابزارهایی که مهاجم استفاده کرده بود، پیچیده نبودند؛ بلکه نقطه نفوذ از طریق فریب روانی و مهندسی اجتماعی حاصل شده بود.

این حمله با روشی ساده و کم‌هزینه، به یکی از بزرگ‌ترین شرکت‌های مالی منطقه آسیب جدی وارد کرد. جالب است بدانید که طبق بررسی‌ها، تنها اگر مریم دقت می‌کرد که دامنه اصلی شرکت چیست یا از احراز هویت دومرحله‌ای استفاده شده بود، این حمله به‌سادگی دفع می‌شد.

راهکارهای پیشگیرانه:

- آموزش مستمر کارکنان درباره فیشینگ، بررسی دامنه، و تشخیص ایمیل‌های جعلی
- استفاده اجباری از احراز هویت دومرحله‌ای برای تمام سرویس‌های سازمانی
- فعال‌سازی فیلترهای دقیق ضد فیشینگ در سیستم ایمیل سازمانی
- محدود کردن دسترسی کاربران به فایل‌ها و منابع حساس
- بررسی و تحلیل مستمر لاگ‌های ورود و فعالیت کاربران

امنیت سایبری فقط به فایروال و آنتی‌ویروس محدود نمی‌شود. در مرکز هر سیستم امن، «رفتار انسان» قرار دارد. اگر کارکنان یک سازمان آموزش ندیده باشند، حتی ساده‌ترین حمله می‌تواند به بحرانی گسترده منجر شود. آگاهی، اولین لایه دفاعی در برابر حملات دیجیتال است – و گاهی، مؤثرترین.



نکات ویژه •••

تهدیدات فیزیکی در امنیت سایبری وقتی در اصلی باز می‌ماند

در بسیاری از بحث‌های امنیت سایبری، تمرکز صرف بر تهدیدات دیجیتال است؛ از فیشینگ و بدافزار گرفته تا حملات DDoS و نفوذ از راه دور. اما در حالی که دیوارهای دیجیتال روز به روز مستحکم‌تر می‌شوند، اغلب ساده‌ترین راه نفوذ همان راهی‌ست که جلوی چشم ماست: دنیای واقعی. تهدیدات فیزیکی، اگرچه کمتر به آن‌ها پرداخته می‌شود، همچنان یکی از مسیرهای مؤثر برای حمله به زیرساخت‌های دیجیتال است. در این مقاله، به‌صورت جامع به انواع حملات فیزیکی، سناریوهای واقعی، اشتباهات رایج و راهکارهای مقابله‌ای می‌پردازیم.

01

تهدیدات فیزیکی چیستند؟

تهدید فیزیکی به هرگونه دسترسی غیرمجاز به زیرساخت‌های سخت‌افزاری، فضاهای کاری، تجهیزات یا اطلاعات از طریق حضور فیزیکی اطلاق می‌شود. برخلاف حملات سایبری که از طریق شبکه انجام می‌شوند، حملات فیزیکی به‌صورت مستقیم از طریق ورود به ساختمان، دسترسی به سرورها، دستکاری تجهیزات، یا حتی مشاهده اطلاعات قابل‌دید در محیط صورت می‌گیرند.

نمونه‌هایی از تهدیدات فیزیکی:

- اتصال فلش‌مموری آلوده به سیستم‌های سازمانی
- دسترسی به لپ‌تاپ رهاشده روی میز بدون قفل شدن
- عکس‌برداری از اطلاعات محرمانه روی مانیتور
- ورود غیرمجاز به اتاق سرور یا انبار تجهیزات
- گم شدن یا دزدیده شدن تلفن همراه حاوی اطلاعات حساس

02

سناریوهای واقعی از تهدیدات فیزیکی

۱. لپ‌تاپ باز روی میز:

در یک سازمان بین‌المللی، کارمندی پس از پایان ساعت کاری، لپ‌تاپ خود را روشن و باز روی میز رها کرد. در طول شب، کارگر نظافت وارد دفتر شد و از روی کنجکاوی، ایمیل‌های کاری را مرور کرد. چند فایل دانلود شد، یک ایمیل به اشتباه ارسال شد و فردا صبح، مدیر IT مجبور شد کل سامانه را بررسی کند.

۲. USB هدیه‌دار:

در یک نمایشگاه تجاری، یک بازدیدکننده به کارمند غرفه یک فلش تبلیغاتی هدیه داد. فلش حاوی اسکریپت اجرای خودکار بود که پس از اتصال، یک backdoor در سیستم ایجاد کرد. کارمند از ماهیت آن اطلاعی نداشت و سیستم سازمانی آلوده شد.

۳. عکس‌برداری از مانیتور:

در یک کافی‌شاپ، یک کارمند ریموت سازمانی در حال بررسی گزارش مالی شرکت بود. در پشت سر او، فردی با موبایل از صفحه مانیتور عکس گرفت. اطلاعات موجود شامل ارقام حساب، نام مشتریان و پروژه‌های جاری بود.

۴.دستکاری دوربین مداربسته:

در یک پروژه عمرانی، فردی که دسترسی فیزیکی به تجهیزات نظارتی داشت، با دستکاری دوربین مداربسته توانست نقاط کور امنیتی ایجاد کند تا در زمان مشخصی برخی وسایل گران‌قیمت را بدون ثبت تصویری جابه‌جا کند.

۵. کارت شناسایی گم‌شده:

کارت ورود یک کارمند به‌طور اتفاقی در پارکینگ جا ماند. شخصی آن را پیدا کرد و روز بعد وارد ساختمان شد، بدون آن‌که مورد سؤال قرار گیرد. او به چند بخش از شرکت دسترسی پیدا کرد و حتی یک لپ‌تاپ را با خود خارج کرد.

03

اشتباهات رایج در حوزه امنیت فیزیکی

- قفل نکردن سیستم هنگام ترک محل کار
- نگهداری رمز عبور روی کاغذ در کنار مانیتور
- عدم استفاده از فیلتر دید مانیتور در فضاهای عمومی
- استفاده از قفل‌های ساده یا کارت‌های ورود بدون احراز هویت دومرحله‌ای
- بی‌توجهی به پرینت‌ها و مدارک روی میز یا در سطل زباله

04

ارتباط تهدیدات فیزیکی با حملات سایبری

یکی از مهم‌ترین نکاتی که باید در نظر داشت این است که تهدیدات فیزیکی اغلب سکوی پرتابی برای حملات سایبری هستند. بسیاری از حملات دیجیتال، ابتدا با دسترسی فیزیکی به دستگاه، نصب بدافزار، یا سرقت اطلاعات لاگین شروع می‌شوند. یعنی حمله ممکن است از اتاقی در ساختمان شروع شود، اما نتیجه‌اش نفوذ به شبکه جهانی باشد.

همچنین در حملات پیچیده‌تر مانند APTها، مهاجمان از چند مرحله فیزیکی (مانند اتصال USB یا دسترسی به سیستم‌های شبکه‌ای بدون مانیتورینگ) برای آماده‌سازی حمله اصلی استفاده می‌کنند. به همین دلیل، امنیت سایبری بدون امنیت فیزیکی یک زنجیره ناقص است.

05

راهکارهای مقابله با تهدیدات فیزیکی

- آموزش کاربران درباره اهمیت قفل کردن سیستم در زمان ترک میز
- ممنوعیت استفاده از USB ناشناس و غیربررسی‌شده
- نصب فیلترهای دید جانبی روی مانیتورها در فضاهای عمومی
- نظارت بر ورود و خروج فیزیکی افراد با ثبت دقیق
- استفاده از سیستم‌های شناسایی دو مرحله‌ای (کارت + اثر انگشت یا رمز پویا)
- قفل‌گذاری فیزیکی روی کیس سرورها و تجهیزات حساس
- استفاده از نرم‌افزارهای ردیابی در لپ‌تاپ‌ها و گوشی‌های کاری
- فرهنگ‌سازی درباره پاک‌سازی امن پرینت‌ها و اسناد کاغذی

در دنیایی که بخش زیادی از امنیت بر پایه دیوارهای مجازی بنا شده، گاهی یک درِ فیزیکی باز می‌تواند همان‌قدر خطرناک باشد که یک پورت باز در شبکه. امنیت فیزیکی باید در کنار امنیت سایبری دیده شود، چرا که بدون اولی، دومی در معرض خطر قرار می‌گیرد. برای رسیدن به یک سیستم ایمن، باید هم دیوار دیجیتال و هم درِ ورودی فیزیکی را محکم بست.

CHECKLIST

... چک‌لیست

۱۰ اقدام فوری برای افزایش امنیت دیجیتال

امنیت دیجیتال، موضوعی نیست که تنها در سطح سازمان‌ها یا بین متخصصان IT مطرح باشد. هر کاربری که از اینترنت استفاده می‌کند – چه برای کار، چه برای سرگرمی – در معرض تهدیدات سایبری قرار دارد. خوشبختانه با رعایت چند اقدام ساده ولی مؤثر، می‌توان تا حد زیادی از این تهدیدات جلوگیری کرد. در این مقاله، ۱۰ اقدام فوری و کاربردی را بررسی می‌کنیم که هر کسی می‌تواند برای ارتقای امنیت دیجیتال خود انجام دهد.

01 استفاده از رمزهای عبور قوی و غیرتکراری

رمز عبور باید حداقل ۱۲ کاراکتر داشته باشد و شامل حروف بزرگ، کوچک، اعداد و نمادها باشد. استفاده از یک رمز برای چند حساب، اشتباهی مرگبار است. بهتر است از ابزارهای مدیریت رمز عبور مانند Bitwarden یا 1Password برای نگهداری رمزها استفاده کنید.

02 فعال‌سازی احراز هویت دومرحله‌ای (2FA)

با فعال کردن احراز هویت دومرحله‌ای برای حساب‌های مهم مانند ایمیل، شبکه‌های اجتماعی و سرویس‌های مالی، حتی اگر رمز عبور شما فاش شود، ورود به حساب بدون کد دومرحله‌ای امکان‌پذیر نیست. برنامه‌هایی مانند Google Authenticator یا Authy در این زمینه بسیار کارآمدند.

03 به‌روزرسانی مداوم سیستم و نرم‌افزارها

سیستم‌عامل، مرورگر و اپلیکیشن‌های نصب‌شده باید همیشه به‌روز باشند. به‌روزرسانی‌ها اغلب برای رفع حفره‌های امنیتی ارائه می‌شوند. تأخیر در نصب آن‌ها می‌تواند راه نفوذ مهاجمان را باز کند.

04 کلیک نکردن روی لینک‌های مشکوک

ایمیل‌های ناشناس، پیامک‌های عجیب و لینک‌هایی که با عنوان‌هایی مانند «شما برنده شدید» ارسال می‌شوند، اغلب دربردارنده فیشینگ هستند. قبل از کلیک، نشانی لینک را بررسی کنید و در صورت شک، آن را نادیده بگیرید.

05 استفاده از آنتی‌ویروس معتبر و فعال بودن فایروال

یک آنتی‌ویروس قابل اعتماد می‌تواند بسیاری از تهدیدات اولیه را شناسایی و خنثی کند. در کنار آن، فایروال سیستم‌عامل باید فعال باشد تا از ورود غیرمجاز جلوگیری شود.

06 استفاده از VPN در وای‌فای عمومی

در مکان‌هایی مانند کافی‌شاپ، هتل یا فرودگاه که وای‌فای عمومی ارائه می‌شود، استفاده از VPN بسیار مهم است. VPN اطلاعات ارسالی شما را رمزنگاری کرده و مانع از استراق سمع می‌شود.

07 قفل کردن دستگاه هنگام ترک میز

چه در محل کار باشید و چه در منزل یا مکان عمومی، هنگام ترک دستگاه حتماً آن را قفل کنید. در سیستم‌های ویندوز می‌توان با کلیدهای میانبر Win+L این کار را انجام داد. قفل کردن موبایل با اثر انگشت یا رمز نیز الزامی است.

08 استفاده از مرورگرهای امن و افزونه‌های حفاظتی

مرورگرهایی مانند Firefox و Brave امکانات امنیتی بیشتری ارائه می‌دهند. افزونه‌هایی مانند uBlock Origin، HTTPS Everywhere و Privacy Badger نیز می‌توانند ردیاب‌ها و کدهای مشکوک را مسدود کنند.

09 مراقبت از اطلاعات در فضای ابری

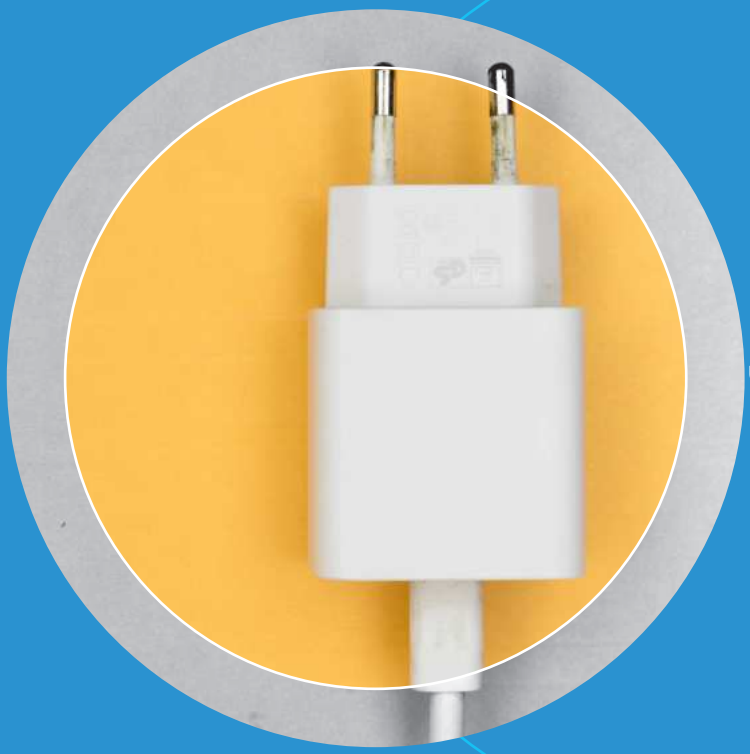
سرویس‌های ابری مانند Google Drive و Dropbox اگرچه کاربردی‌اند، اما باید با رمز عبور قوی و 2FA ایمن شوند. همچنین فایل‌های حساس را با رمزگذاری (encryption) بارگذاری کنید و اشتراک‌گذاری عمومی را غیرفعال نمایید.

10 آموزش و آگاهی مستمر

امنیت دیجیتال یک فرایند ایستا نیست. تهدیدات روزبه‌روز تغییر می‌کنند. دنبال کردن منابع معتبر، شرکت در دوره‌های کوتاه آنلاین یا حتی مطالعه مقاله‌های ساده درباره امنیت، می‌تواند آگاهی شما را بالا نگه دارد و رفتارهای اشتباه را اصلاح کند.

STORY SCENARIO

سناریوی داستانی



وقتی یک شارژر ساده شبکه سازمانی را زمین زد

همه‌چیز از یک روز عادی کاری شروع شد. شرکت مهندسی «آراد دیتا»، فعال در زمینه طراحی سامانه‌های کنترل صنعتی، در تدارک ارائه طرحی مهم به یکی از مشتریان دولتی بود. سالن جلسات در طبقه پنجم آماده ارائه بود، مدیر پروژه‌ها در اتاق کنفرانس جلسه‌ای فشرده داشت، و تیم فنی درگیر هماهنگی آخرین نسخه فایل‌های طراحی شده بودند. در همین شلوغی و رفت‌وآمدها، یک شیء کوچک و به‌ظاهر بی‌اهمیت جا مانده بود: شارژر یک گوشی موبایل.

شارژر روی میز کنار پریز برق بود. رنگش مشکی و مارک‌دار. کسی توجهی به آن نکرد. شاید از همکار قبلی مانده بود. اما واقعیت این بود که هیچ‌کس از اعضای تیم آن را نمی‌شناخت.

چند ساعت بعد، علی (کارشناس جوان بخش طراحی) پس از بازگشت از جلسه، متوجه شد باتری موبایلش در حال تمام شدن است و نیاز فوری به تماس با واحد پشتیبانی یک تأمین‌کننده خارجی دارد. شارژر خودش را در دفتر فراموش کرده بود. همان لحظه شارژر روی میز را دید و با خوشحالی گفت: «عالیه، همینو بزنم تا تماس بگیرم.»

او شارژر را به گوشی‌اش متصل کرد و هم‌زمان برای بررسی اسناد پروژه به سیستمش بازگشت. اما آنچه نمی‌دانست، این بود که این شارژر معمولی نبود. درون آداپتور، یک ماژول سخت‌افزاری کوچک تعبیه شده بود که پس از اتصال، به‌عنوان یک کیبورد HID شناسایی می‌شد و ظرف چند ثانیه، مجموعه‌ای از دستورات را روی سیستم علی اجرا کرد. بدون صدا، بدون پنجره، بدون هیچ اثری ظاهری.

اسکریپت اولیه، تنها یک بدافزار سبک را از یک سرور خارجی بارگیری و نصب کرد. این بدافزار پس از اجرا، شروع به جمع‌آوری داده‌های کاربر، رمزهای ذخیره‌شده، توکن‌های لاگین، مسیرهای دسترسی و حتی لاگ فعالیت‌های روزانه کرد. سپس ارتباطی رمزگذاری‌شده با مرکز فرمان مهاجم برقرار کرد و منتظر دستورات بعدی شد.

تا اینجا، علی حتی متوجه چیزی نشده بود. تلفن خود را جدا کرد، تماس گرفت و ادامه روزش را مثل همیشه گذراند. اما در پس‌زمینه، مهاجم حالا یک پایگاه نفوذ قدرتمند داخل شبکه آراد دیتا داشت.

روز دوم، فعالیت‌ها شدت گرفت. مهاجم از طریق بدافزار، توانست لیست دسترسی‌های Active Directory را مشاهده کند. چون سیستم علی در پروژه‌های طراحی صنعتی با فایل‌های CAD در تعامل بود، دسترسی‌هایی به فولدرهای مشترک پروژه‌ها داشت. مهاجم از این مسیر وارد پوشه‌ای شد که شامل نسخه اولیه طراحی‌های یک پروژه حساس برای زیرساخت آب‌رسانی شهری بود. فایل‌ها استخراج شدند و بدون دست‌کاری مستقیم، در سامانه‌ای ناشناس آپلود شدند. اما هدف تنها سرقت اطلاعات نبود؛ نفوذ به‌صورت تدریجی در حال گسترش بود. هکر، اسکریپت‌هایی برای بررسی دیگر سیستم‌های روی همان Subnet اجرا کرد و از طریق آسیب‌پذیری SMBv۱ در یکی از سیستم‌های قدیمی‌تر، به سرور محلی فایل دسترسی یافت.

روز سوم، سیستم‌های شرکت شروع به بروز نشانه‌های عجیب کردند: دسترسی به بعضی فایل‌ها قطع شد، برخی از اسناد به‌طور ناگهانی حجم‌شان تغییر کرد و سیستم گزارش‌دهی داخلی با خطا مواجه شد. تیم IT وارد عمل شد. ابتدا تصور شد اختلال نرم‌افزاری یا اشکال در پیکربندی شبکه است. اما در بررسی لاگ‌ها، ورودهایی از یک سیستم ناشناخته در داخل شبکه شناسایی شد.

با تحقیقات بیشتر، معلوم شد آدرس MAC سیستم علی با چند آی‌پی مختلف در ساعات غیرعادی فعالیت داشته. و وقتی علی مطلع شد که یکی از مدیران پروژه فایلی را در اختیار دارد که خودش هیچ‌وقت ارسال نکرده، حدس اولیه تیم امنیت تأیید شد: یک نفوذ جدی اتفاق افتاده.

تیم امنیت به‌سرعت شبکه داخلی را ایزوله کرد. سیستم‌های آلوده از شبکه جدا شدند. ترافیک به‌صورت آفلاین تحلیل شد و مسیر ورود اولیه شناسایی شد: همان شارژر.

از طریق دوربین‌های مدار بسته، بررسی شد چه کسی در آن بازه زمانی وارد اتاق جلسات شده بود. فردی با ظاهر رسمی که برای جلسه معرفی محصول وارد ساختمان شده بود، و طبق روال امنیتی پایین ساختمان، فقط ثبت نام انجام داده بود، نه احراز هویت کامل. او پس از خروج، دیگر دیده نشد.

نتایج حمله:

- چهار سیستم آلوده به بدافزار شناسایی شد
- فایل‌های کلیدی طراحی پروژه به بیرون نشت کرد
- یکی از قراردادهای کلیدی به حالت تعلیق درآمد چون مشتری درباره محرمانگی پروژه دچار تردید شد
- شرکت مجبور به بازبینی کامل سیاست‌های امنیت فیزیکی و سایبری شد
- تمامی ورودی‌های فیزیکی ملزم به احراز هویت دو مرحله‌ای شدند

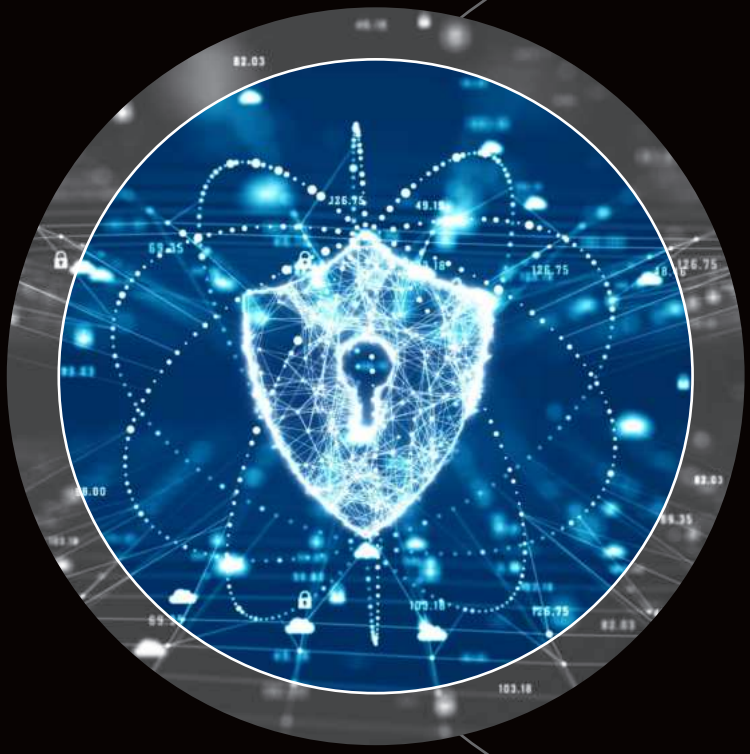
این داستان شاید تخیلی به‌نظر برسد، اما تکنولوژی BadUSB و شارژرهای آلوده، واقعیتی کاملاً مستند در دنیای امنیت اطلاعات هستند. حمله‌هایی با همین سبک، بارها در سازمان‌های مهم جهان اتفاق افتاده‌اند.

درس‌هایی که باید گرفت:

- هر دستگاهی که به سیستم متصل می‌شود، یک تهدید بالقوه است، حتی شارژر
- امنیت فیزیکی بخشی از امنیت سایبری است و نباید جدا دیده شود
- سیاست‌های Zero Trust باید در سطوح سخت‌افزاری هم اجرا شوند
- کارمندان باید درباره ابزارهای آلوده، آموزش ببینند

امنیت یعنی مراقب باشیم چه چیزی به چه چیزی وصل می‌شود. گاهی، یک کابل ساده می‌تواند کل شبکه را به زانو درآورد.

SECURITY GLOSSARY



واژه‌نامه امنیتی

واژه‌های مهم دنیای امنیت به زبان ساده

در دنیای پرسرعت و پیچیده امروز، واژه‌های تخصصی دنیای امنیت سایبری ممکن است برای بسیاری از کاربران گیج‌کننده باشد. اما آشنایی با این واژه‌ها می‌تواند به ما کمک کند تا تهدیدات را بهتر بشناسیم، تصمیم‌های هوشمندانه‌تری بگیریم، و رفتار دیجیتال امن‌تری داشته باشیم. در این بخش از ماهنامه، مجموعه‌ای از مهم‌ترین اصطلاحات امنیتی را به زبان ساده و قابل فهم برای کاربران غیر فنی گردآوری کرده‌ایم. این واژه‌نامه نه تنها برای کاربران عادی بلکه برای مدیران، کارمندان، و حتی والدینی که می‌خواهند از فرزندان‌شان در فضای مجازی محافظت کنند، مفید است.

01

حمله زنجیره تأمین
(Supply Chain Attack)

وقتی مهاجمان به‌جای حمله مستقیم به هدف نهایی، به یکی از شرکت‌های واسط یا تأمین‌کننده نرم‌افزار یا خدمات حمله می‌کنند. نمونه معروف آن حمله به شرکت SolarWinds است که به واسطه شرکت مایکروسافت و بسیاری از شرکت‌های معتبر حوزه فناوری اطلاعات بواسطه آن هک شدند.

02

پایش تهدید
(Threat Monitoring)

فرایندی مداوم برای شناسایی فعالیت‌های مشکوک یا غیرعادی در سیستم‌ها و شبکه‌ها، که هدف آن تشخیص زودهنگام حملات احتمالی است.

03

تحلیل رفتاری
(Behavioral Analysis)

روشی برای شناسایی تهدیدات بر اساس رفتار کاربران یا سیستم‌ها، نه فقط امضای بدافزارها. به‌ویژه برای شناسایی حملات ناشناخته مفید است.

04

تهدید داخلی
(Insider Threat)

وقتی خطر از درون سازمان می‌آید، مثلاً کارمندی ناراضی یا بی‌احتیاط، به‌صورت عمدی یا سهوی اطلاعاتی را فاش می‌کند یا آسیب می‌زند.

05

امنیت سایبری مبتنی بر هویت
(Identity-based Security)

رویکردی نوین در امنیت که تمرکز آن به‌جای سیستم‌ها، روی کاربران و هویت دیجیتال آن‌هاست. مثل استفاده از احراز هویت چندمرحله‌ای، بررسی سطح دسترسی و رفتارشناسی کاربر.

06

باج‌افزار
(Ransomware)

نوعی بدافزار که فایل‌های سیستم را رمزگذاری می‌کند و برای بازگرداندن آن‌ها درخواست پول می‌کند.

07

آنتی‌ویروس
(Antivirus)

نرم‌افزاری که سیستم را اسکن می‌کند و جلوی اجرای بدافزارها را می‌گیرد. به‌روز بودن آنتی‌ویروس اهمیت زیادی دارد.

08

دیواره آتش
(Firewall)

نوعی فیلتر دیجیتال که تصمیم می‌گیرد کدام ارتباط‌ها اجازه ورود به سیستم یا شبکه را داشته باشند و کدام نه.

09

وای‌فای عمومی
(Public Wi-Fi)

شبکه‌های وای‌فای باز در مکان‌هایی مثل کافی‌شاپ‌ها یا فرودگاه‌ها. اغلب ناامن هستند و بهتر است در آن‌ها از VPN استفاده شود.

10

VPN
(Virtual Private Network)

ابزاری برای رمزنگاری ارتباطات اینترنتی. باعث می‌شود اطلاعات شما در مسیر بین دستگاه شما و اینترنت قابل مشاهده نباشد.

11

بروزرسانی امنیتی
(Security Update)

پچ‌هایی که شرکت‌های نرم‌افزاری برای رفع حفره‌های امنیتی منتشر می‌کنند. نصب نکردن آن‌ها می‌تواند به نفوذ هکرها منجر شود.

12

نشت اطلاعات
(Data Breach)

زمانی که اطلاعات خصوصی یا حساس کاربران به‌صورت عمدی یا تصادفی از دسترس خارج شده یا منتشر شود.

13

رمزنگاری
(Encryption)

فرایند تبدیل اطلاعات به کدی نامفهوم، به‌طوری‌که فقط با کلید مخصوص قابل خواندن باشد. در پیام‌رسان‌ها و سایت‌های بانکی کاربرد زیادی دارد.

14

حمله مرد میانی
(MITM)

وقتی هکری بین شما و سایت مورد نظر قرار می‌گیرد و اطلاعات ردوبدل شده را مشاهده یا دست‌کاری می‌کند. معمولاً در وای‌فای‌های ناامن اتفاق می‌افتد.

15

پورت باز
(Open Port)

دروازه‌هایی در شبکه که برای ارتباط با سرویس‌های مختلف باز می‌مانند. اگر کنترل نشوند، راه ورود مهاجمان هستند.

16

سیاست رمز عبور
(Password Policy)

مجموعه‌ای از قوانین برای ساخت و مدیریت رمزهای عبور، مثل طول رمز، عدم تکرار و دوره‌ای بودن تغییر رمز.

17

لینک مخرب
(Malicious Link)

لینک‌هایی که با کلیک روی آن‌ها، سیستم آلوده می‌شود یا اطلاعات شما به سرقت می‌رود. اغلب در ایمیل‌ها و پیام‌ها پنهان می‌شوند.

18

لاگین جعلی
(Fake Login Page)

صفحه‌هایی که کاملاً شبیه صفحه ورود سایت‌های اصلی هستند ولی اطلاعات وارد شده را برای هکر می‌فرستند.

19

دسترسی غیرمجاز
(Unauthorized Access)

زمانی که فردی بدون اجازه وارد حساب، سیستم یا شبکه‌ای شود.

20

نرم‌افزارهای کرک‌شده
(Cracked Software)

نرم‌افزارهایی که بدون مجوز قانونی استفاده می‌شوند. اغلب حاوی بدافزار یا در پشتی هستند و امنیت سیستم را تهدید می‌کنند.

شناخت واژه‌های پایه‌ی امنیت سایبری، اولین قدم برای محافظت بهتر در دنیای دیجیتاله. این واژه‌نامه ساده، شروع خوبی برای آشنایی با امنیت به‌عنوان بخشی از زندگی روزمره‌ست، نه یه چیز ترسناک یا پیچیده.

INTRODUCTION OF SOURCES

... معرفی منابع

منابع پیشنهادی برای یادگیری بیشتر

در دنیای امنیت سایبری، یادگیری هیچ‌وقت تمام نمی‌شود. تهدیدها هر روز پیچیده‌تر می‌شوند و دانستنِ بیشتر، یعنی محافظت بهتر. در این بخش، منابعی کاربردی و معتبر برای یادگیری بیشتر امنَیت دیجیتال معرفی می‌کنیم. این منابع برای همه مفید هستند: چه تازه‌کار باشید، چه علاقه‌مند، یا حتی متخصصی که به‌دنبال به‌روز ماندن است.

کتاب‌های فارسی

امنیت اطلاعات به زبان ساده – علی قائمی کتابی فارسی برای مبتدیان که مفاهیم پایه‌ای امنیت را به‌طور قابل‌فهم و کاربردی توضیح می‌دهد. مناسب برای کاربران عمومی و اداری.

امنیت شبکه‌های کامپیوتری – نویسنده: دکتر فرهاد زندیه کتابی دانشگاهی که اصول امنیت شبکه، رمزنگاری و مدیریت تهدیدات را به زبان علمی و کاربردی آموزش می‌دهد.

راهنمای امنیت دیجیتال برای فعالان مدنی – ترجمه کمیته آموزش دیجیتال کلیک راهنمایی مفید برای افراد و گروه‌هایی که با اطلاعات حساس یا در معرض ریسک کار می‌کنند.

پادکست‌ها و کانال‌های ایرانی

پادکست رادیو امنیت که در حوزه اخبار، تحلیل و بررسی حملات گوناگون در حوزه امنیت اطلاعات و توسط گروه لیان تدوین و ارائه می‌شود.

پادکست سکانس صفر (SecZero) پادکستی فارسی در زمینه امنیت اطلاعات و تحلیل رخدادهای امنیتی با نگاهی فنی و تخصصی اما قابل فهم برای علاقه‌مندان عمومی.

پادکست رادیو جادی که توسط امیر میرمیرانی تهیه و تدوین می‌شود که به بررسی مباحث روز دنیای امنیت دیجیتال پرداخته و آنها را زوایای مختلف بررسی می‌کند.

در دنیای پرخطر دیجیتال، دانستن قدرت است. با کمک این منابع فارسی، می‌توانید از مفاهیم پایه تا نکات کاربردی امنیت دیجیتال را بیاموزید و از خودتان، خانواده‌تان یا حتی سازمان‌تان بهتر محافظت کنید. فقط کافیه از یکی شروع کنید!