24th International Conference on Information Technology, Computer and Telecommunication
بیست و چهارمین کنفرانس بین المللی فناوری اطلاعات، کامپیوتر و مخابرات | گرجستان
Event Place: Tbilisi,Georgia
www.itctconf.ir
24th International Conference on Information Technology,Computer and Telecommunication

(آسیب‌پذیری‌های سایبری در شرکت‌ها و روش‌های عملی برای جلوگیری از آن‌ها)

محراب فراغتی

پژوهشگر حوزه امنیت شبکه های کامپیوتری

چکیده:

در عصر دیجیتال، تهدیدات سایبری به یکی از مهم‌ترین چالش‌های پیش روی شرکت‌ها و سازمان‌ها تبدیل شده‌اند. با ظهور انواع جدیدی از حملات سایبری نظیر باج‌افزارها، مهندسی اجتماعی، تهدیدات داخلی و حملات زنجیره تأمین، شرکت‌ها با خطرات گسترده‌ای روبه‌رو هستند که می‌توانند منجر به از دست رفتن اطلاعات حساس و خسارت‌های مالی قابل توجه شوند. این مقاله با بررسی این تهدیدات نوین و تحلیل روش‌های دفاعی شرکت‌ها، راهکارهایی برای مقابله با این خطرات پیشنهاد می‌دهد. با استفاده از آموزش کارکنان، پیاده‌سازی نرم‌افزارهای امنیتی، رمزنگاری اطلاعات، بکاپ‌گیری منظم و همکاری با مشاوران امنیت سایبری، شرکت‌ها می‌توانند به تقویت امنیت سیستم‌های خود بپردازند. این استراتژی‌ها

•به شرکت‌ها کمک می‌کند تا مقاومت بیشتری در برابر حملات سایبری داشته باشند

مقدمه:

امنیت سایبری به یکی از مسائل مهم و حیاتی برای کسب‌وکارها تبدیل شده است. با گسترش فناوری و افزایش وابستگی سازمان‌ها به فضای دیجیتال، میزان و تنوع حملات سایبری نیز به شکل چشمگیری افزایش یافته است. طبق گزارش‌های اخیر، شرکت‌ها به‌طور مداوم در معرض حملات جدید و پیچیده‌ای قرار دارند که می‌تواند تهدید جدی برای فعالیت‌های روزمره آن‌ها محسوب شود.

تهدیدات سایبری نه تنها باعث از دست رفتن داده‌ها و اطلاعات حیاتی می‌شوند، بلکه می‌توانند شهرت و اعتماد عمومی به سازمان‌ها را نیز تحت تأثیر قرار دهند. از جمله تهدیدات جدیدی که شرکت‌ها با آن‌ها مواجه هستند می‌توان به حملات باج‌افزار، مهندسی اجتماعی، تهدیدات داخلی و حملات زنجیره تأمین اشاره کرد. این تهدیدات به دلیل پیچیدگی و پتانسیل تخریب بالا، سازمان‌ها را مجبور به اتخاذ رویکردهای جدید و متنوعی برای حفاظت از اطلاعات و زیرساخت‌های خود کرده‌اند.

این مقاله به بررسی این تهدیدات سایبری جدید و روش‌های دفاعی مورد استفاده توسط شرکت‌ها می‌پردازد. هدف اصلی این مقاله ارائه یک نمای کلی از تهدیدات موجود و معرفی استراتژی‌های مختلف مقابله با آن‌ها است تا به شرکت‌ها و سازمان‌ها کمک کند در برابر این تهدیدات آمادگی بیشتری داشته باشند.

تهدیدات سایبری جدید

1. حملات باج‌افزار (Ransomware Attacks)

حملات باج‌افزار از رایج‌ترین تهدیدات سایبری به‌شمار می‌آیند. در این حملات، مهاجم یک بدافزار را به سیستم قربانی وارد کرده و داده‌ها را رمزگذاری می‌کند و دسترسی به داده‌ها تنها با پرداخت باج به مهاجم ممکن است .

روش‌های انتشار: مهاجمان معمولاً از طریق پیوست‌های ایمیل‌های مشکوک، لینک‌های آلوده و سایت‌های ناامن باج‌افزار را منتشر می‌کنند. همچنین، این نوع حملات می‌توانند از طریق آسیب‌پذیری‌های نرم‌افزاری یا شبکه‌ای نیز نفوذ کنند.

نمونه‌های واقعی: یکی از شناخته‌شده‌ترین نمونه‌های حمله باج‌افزار، حمله "وناکرای (WannaCry)" بود که در سال ۲۰۱۷ رخ داد و هزاران سیستم در سراسر جهان را تحت تأثیر قرار داد. این حمله خسارت‌های گسترده‌ای به سازمان‌های مختلف وارد کرد و نیاز به به‌روزرسانی فوری نرم‌افزارها را برجسته ساخت.

2.حملات مهندسی اجتماعی (Social Engineering Attacks)

حملات مهندسی اجتماعی شامل تکنیک‌هایی می‌شوند که به جای هک کردن سیستم، افراد را هدف قرار می‌دهند. مهاجم تلاش می‌کند از طریق فریب دادن کارکنان یا کاربران، اطلاعاتی مانند رمز عبور یا اطلاعات مالی را به دست آورد.

- روش‌ها: رایج‌ترین روش مهندسی اجتماعی فیشینگ (Phishing) است، که در آن مهاجم یک ایمیل به ظاهر قانونی را برای قربانی ارسال می‌کند و از او می‌خواهد اطلاعات حساسی را ارائه دهد. روش‌های دیگر شامل وی‌شینگ (Vishing) و اس‌ام‌اس فیشینگ (Smishing) می‌باشند.

- نمونه‌ها: یکی از نمونه‌های مشهور حملات فیشینگ، حمله به سرویس ایمیل "Gmail" بود که موجب دسترسی غیرمجاز به اطلاعات کاربران شد. این حملات نشان‌دهنده ضعف در تشخیص پیام‌های تقلبی توسط کارکنان است.

3.تهدیدات داخلی (Insider Threats)

تهدیدات داخلی زمانی رخ می‌دهند که یکی از کارکنان یا پیمانکاران فعلی یا سابق، به دلایل مختلف مانند نارضایتی، عمداً یا غیرعمدی به اطلاعات شرکت دسترسی غیرمجاز پیدا می‌کند و از آن‌ها سوءاستفاده می‌کند.

- انواع تهدیدات داخلی**: برخی از کارکنان ممکن است به طور غیرمستقیم و بدون اطلاع امنیت شرکت را به خطر بیندازند، در حالی که دیگران ممکن است به عمد از اطلاعات سوءاستفاده کنند. همچنین، کارکنانی که دسترسی‌های غیرضروری دارند، ریسک بالایی را ایجاد می‌کنند.

- مثال‌ها: مواردی از این تهدیدات شامل افشای اطلاعات حساس یا فروش اطلاعات مشتریان به رقبا است.

4.حملات زنجیره تأمین (Supply Chain Attacks)

در این نوع حملات، مهاجمان از ضعف‌های موجود در سیستم‌های تأمین‌کنندگان یا شرکای تجاری استفاده می‌کنند و از طریق آن‌ها به شبکه اصلی شرکت دسترسی پیدا می‌کنند.

- شیوه عملکرد: مهاجمان با شناسایی نقاط ضعف امنیتی در نرم‌افزارها یا خدماتی که شرکت استفاده می‌کند، این نقاط را مورد سوءاستفاده قرار می‌دهند. بدافزار یا دسترسی‌های غیرمجاز می‌تواند از طریق تأمین‌کنندگان به سیستم‌های شرکت وارد شود.

نمونه‌ها: حمله به شرکت "SolarWinds" در سال ۲۰۲۰ یکی از بزرگترین حملات زنجیره تأمین بود که از طریق یک آپدیت آلوده به بدافزار، هزاران مشتری را تحت تأثیر قرار داد.

روش‌های دفاعی شرکت‌ها

1.آموزش کارکنان و افزایش آگاهی

-- بسیاری از حملات، به ویژه حملات مهندسی اجتماعی، به دلیل عدم آگاهی کارکنان صورت می‌گیرد. شرکت‌ها برنامه‌های آموزشی برگزار می‌کنند تا سطح آگاهی امنیتی کارکنان خود را ارتقاء دهند.

--محتوای آموزشی: این آموزش‌ها شامل نحوه تشخیص ایمیل‌های فیشینگ، عدم به اشتراک‌گذاری اطلاعات حساس، و رعایت اصول امنیتی در کار با سیستم‌ها است.

--کارگاه‌های عملی: شرکت‌ها ممکن است کارگاه‌هایی با شبیه‌سازی حملات برگزار کنند تا کارکنان در شرایط واقعی نحوه برخورد با تهدیدات را تمرین کنند.

2.نرم‌افزارهای امنیتی و سامانه‌های حفاظتی

استفاده از ابزارهای امنیتی مانند فایروال‌ها، آنتی‌ویروس‌ها، و سامانه‌های تشخیص نفوذ (IDS) به شرکت‌ها کمک می‌کند تا حملات را در مراحل ابتدایی شناسایی و خنثی کنند.

- انواع نرم‌افزارهای امنیتی: از جمله ابزارهای مهم می‌توان به نرم‌افزارهای مدیریت اطلاعات و رویدادهای امنیتی (SIEM) اشاره کرد که به تحلیل و شناسایی الگوهای مشکوک در سیستم‌ها کمک می‌کنند.

- پایش مداوم شبکه: سامانه‌های IDS و IPS (سیستم‌های جلوگیری از نفوذ) به صورت مداوم شبکه را پایش می‌کنند و به محض شناسایی فعالیت‌های مشکوک، اقدامات لازم را انجام می‌دهند.

3.رمزنگاری و کنترل دسترسی‌ها

برای حفاظت از اطلاعات حساس، بسیاری از شرکت‌ها از سیستم‌های رمزنگاری پیشرفته و پروتکل‌های کنترل دسترسی استفاده می‌کنند.

- رمزنگاری اطلاعات**: استفاده از رمزنگاری قوی برای اطلاعات در حال انتقال و در حالت ذخیره شده، یکی از راه‌های مؤثر برای حفاظت از اطلاعات است.

- مدیریت هویت و دسترسی (IAM): این سیستم‌ها به شرکت‌ها اجازه می‌دهند تا دسترسی کارکنان به اطلاعات حساس را کنترل کرده و دسترسی‌های اضافی را محدود کنند.

4.بکاپ‌گیری منظم و ایمن

یکی از راهکارهای کارآمد در مقابله با حملات باج‌افزار، بکاپ‌گیری منظم از داده‌ها است. این بکاپ‌ها باید در یک فضای امن و جداگانه ذخیره شوند تا در صورت نیاز قابل بازیابی باشند.

- سیاست‌های بکاپ‌گیری**: شرکت‌ها معمولاً از سیاست‌های متعددی برای بکاپ‌گیری داده‌ها استفاده می‌کنند. برخی از این سیاست‌ها شامل بکاپ‌های روزانه، هفتگی

و ماهانه می‌باشد.

- ذخیره‌سازی ایمن: بکاپ‌ها باید به‌گونه‌ای ذخیره شوند که حتی در صورت حمله به شبکه اصلی، مهاجمان نتوانند به آن‌ها دسترسی پیدا کنند.

کلمات کلیدی :

تهدیدات سایبری، حملات باج‌افزار، مهندسی اجتماعی، تهدیدات داخلی، حملات زنجیره تأمین، امنیت اطلاعات، بکاپ‌گیری، امنیت سایبری

منابع پیشنهادی:

1. Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man in the middle attacks. IEEE Communications Surveys & Tutorials, 18(3), 2027-2051.

2. Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. International Management Review, 13(1), 10-21.

3. Symantec Corporation. (2019). Internet Security Threat Report. Symantec, Inc.

4. Kaspersky Lab. (2021). The State of Industrial Cybersecurity 2021. Kaspersky Research Report.

5. Verizon. (2022). 2022 Data Breach Investigations Report. Verizon Communications Inc.