ماهنامه برنا

Borna Network Managers
مدیران شبکه برنا

اخبار حوزه امنیت و شبکه (بهمن ۱۴۰۴)

دورکاری در زمان بحران، اگر با رعایت رفتارهای امن در وب، مدیریت درست نرم‌افزارها و دسترسی‌ها، و حفاظت از سیستم‌ها/جلسات آنلاین همراه باشد، می‌تواند بدون افزایش ریسک امنیتی ادامه پیدا کند.
برای کاهش تهدیداتی مثل فیشینگ، بدافزار و نشت اطلاعات، به روزرسانی مداوم، احراز هویت دومرحله‌ای، رمزگذاری داده‌ها و استفاده از ابزارهای امنیتی معتبر (مثل آنتی‌ویروس سازمانی، DLP و PAM) ضروری است. همزمان دو هشدار جدی مطرح است: آسیب‌پذیری بحرانی telnetd در GNU Inetutils با امکان دور زدن احراز هویت و همچنین نشت گسترده اطلاعات ۱۷.۵ میلیون حساب اینستاگرام که ریسک فیشینگ و سوءاستفاده از حساب‌ها را بالا برده است.

ویژه مدیران و کارشناسان شبکه و امنیت

www.bornanetwork.co
info@bornanetwork.co
۰۲۱-۷۴۰۲۸

خبرنامه امنیت سایبری - بهمن ماه

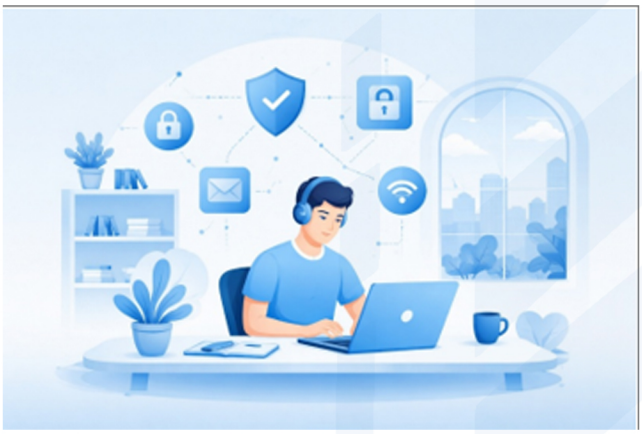
راهنمای امنیتی دورکاری در زمان بحران

دورکاری نه تنها یک گزینه انتخابی بلکه به یکی از پایه های اصلی فعالیت حرفه‌ای تبدیل شده است. با شرایط اقتصادی در سالهای 2020 تا 2025 ، افرادی که پیش‌تر تجربه کار از خانه داشتند، ساعات بیشتری را خارج از محیط‌های اداری سپری کردند و بسیاری برای اولین بار به این سبک کاری روی آوردند. همانند هر مدل کاری دیگر، دورکاری فرصت‌ها و مزایای خاص خود را دارد، اما در عین حال می‌تواند ریسک‌های جدی امنیتی ایجاد کند. رعایت اصول فنی و استانداردهای جهانی، همراه با استفاده از ابزارهای امنیتی مدرن، کلید حفظ امنیت اطلاعات در این شرایط است.

در این راهنمای فنی، توصیه‌ها و الزامات امنیتی دورکاری ارائه شده‌اند که شامل حوزه‌های زیر هستند:

- رعایت رفتارهای امن هنگام مرور وب و استفاده از اینترنت
- حفاظت از سیستم‌ها و تجهیزات شخصی با رویکردهای حرفه‌ای
- مدیریت امن سامانه‌ها، اپلیکیشن‌ها و حساب‌های کاری
- رعایت نکات امنیتی در جلسات آنلاین و همکاری‌های مجازی
- وظایف کلیدی مدیران IT و مسئولان امنیت

رعایت این اصول، در کنار بهره‌گیری از نرم افزارهای امنیتی معتبر مانند ESET Endpoint Security برای محافظت در برابر بدافزار و تهدیدات پیشرفته، Safetica DLP برای پیشگیری از نشت اطلاعات، و PAM Arcon برای مدیریت دسترسی و حساب‌های با دسترسی بالا، تضمین کننده سطح بالای امنیت در محیط دورکاری است.



وب‌گردی امن و مواجهه با تهدیدهای آنلاین

هنگام مرور اینترنت، توجه به آدرس سایت‌ها و منبع فایل‌ها حیاتی است. مهاجمان سایبری معمولاً با ایجاد دامنه‌هایی شبیه به سایت‌های معتبر، کاربران را به صفحات فیشینگ هدایت می‌کنند تا اطلاعات حساس مانند نام کاربری و گذرواژه را جمع‌آوری کنند. این حملات ممکن است از طریق ایمیل، پیامک یا پیام رسان‌ها آغاز شوند و محدود به سامانه‌های بانکی نیستند.

در مواجهه با لینک‌ها یا فایل‌هایی که با عنوان اخبار داغ یا موضوعات حساس منتشر می‌شوند، باید دقت مضاعف داشته باشید. رویدادهای بزرگ جهانی، بحران های اقتصادی یا اخبار شوک‌آور ابزار مناسبی برای فریب کاربران هستند و می‌توانند به نصب بدافزار یا اجرای حملات فیشینگ منجر شوند.

وب‌سایت‌های نامعتبر یا غیرقانونی نیز منبع شایع بدافزارها هستند. این سایت‌ها ممکن است با پیشنهاد دانلود فایل یا پخش ویدئو، نرم‌افزارهای مخرب را به صورت خودکار روی سیستم شما نصب کنند. توصیه می‌شود فایل‌ها و نرم‌افزارها را تنها از منابع رسمی دریافت کنید و قبل از اجرا، آن‌ها را توسط سرویس‌های آنلاین تشخیص بدافزار مانند VirusTotal بررسی کنید. همچنین انجام این فعالیت‌ها روی یک سیستم جدا از محیط کاری توصیه می‌شود.

در صورتی که به صورت ناخواسته ایمیلی به فرد اشتباهی ارسال کردید، روی لینک مشکوک کلیک کردید یا فایل مشکوکی را باز نمودید، فوراً این موضوع را به واحد فناوری اطلاعات یا تیم امنیت اطلاع دهید. گزارش سریع این خطاها از گسترش آسیب جلوگیری کرده و می‌تواند مانع از بروز حادثه‌ای جدی شود.

خبرنامه امنیت سایبری - بهمن ماه

حفظ امنیت سیستم و داده‌ها

• نصب و به‌روزرسانی مداوم نرم‌افزارها و وصله‌های امنیتی (Patch) ضروری است. به‌روزرسانی‌ها آسیب‌پذیری‌های شناخته‌شده را رفع کرده و نفوذ مهاجمان را دشوارتر می‌کنند.

• از انجام فعالیت‌های حساس روی شبکه‌های عمومی و ناامن اجتناب کنید. در صورت استفاده اجتناب‌ناپذیر، حتماً از ارتباطات رمزگذاری‌شده و پروتکل HTTPS بهره ببرید.

• داده‌های محرمانه و فایل‌های حساس مانند اطلاعات مشتریان را رمزگذاری و منتقل کنید. تنها افرادی که کلید رمزگشایی در اختیار دارند، قادر به دسترسی خواهند بود.

• تبادل گذرواژه‌ها یا داده‌های حساس بین اعضای دورکار را محدود کنید و پس از انجام فعالیت، گذرواژه‌ها را تغییر دهید. Safetica DLP می‌تواند در مدیریت و نظارت بر انتقال داده‌های محرمانه بسیار کمک‌کننده باشد.

• استفاده از گذرواژه‌های طولانی و ترکیبی و مدیریت آن ها توسط نرم‌افزارهای مدیریت گذرواژه، امنیت را به شکل قابل توجهی افزایش می‌دهد.

امنیت جلسات و همکاری آنلاین

• وب‌کم را در زمان عدم استفاده پوشانده یا نرم افزاری غیرفعال کنید تا از جاسوسی تصویری جلوگیری شود.

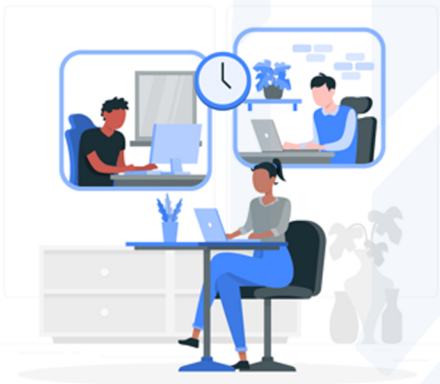
• از ابزارهای جانبی برای جلوگیری از مشاهده صفحه نمایش توسط دیگران بهره ببرید.

• دستگاه‌ها را در اختیار افراد غیرمرتبط قرار ندهید.

• سیستم را هنگام ترک محل یا تماس‌های کاری قفل کنید و ویژگی قفل خودکار را فعال نمایید.

• هنگام اشتراک‌گذاری صفحه نمایش، مراقب اطلاعات محرمانه و نمای برنامه‌های نصب‌شده باشید.

• فایل‌ها و لینک‌های دریافتی را پیش از استفاده اسکن کنید. استفاده از ESET Endpoint Security می‌تواند بدافزارهای ناشناخته را شناسایی کند.



خبرنامه امنیت سایبری - بهمن ماه

وظایف مدیران IT و مسئولان امنیت

• در تعطیلات یا شرایط بحرانی، فعالیت هکرها و باج افزارها افزایش می‌یابد. شبکه را به طور مداوم نظارت کنید و فعالیت‌های مشکوک را ردیابی نمایید.
• اطلاع‌رسانی به مدیر ارشد باید از طریق کانال‌های امن و در شرایط اضطرار از پیام‌رسان‌های عمومی انجام شود.
• نسخه چاپی چک‌لیست‌های امنیتی را در مکانی امن نگه دارید تا در هر بار دورکاری همه اصول رعایت شوند.
• از ذخیره‌سازی ابری خارجی در صورت احراز هویت امن و پشتیبانی از تایید دو مرحله‌ای استفاده کنید.
• ابزارهای کنترل دسترسی (Access Control) و VPN برای کاربران دورکار، دسترسی امن و خصوصی را تضمین می‌کنند.
• استفاده از PAM Arcon برای مدیریت حساب‌های با دسترسی بالا و کنترل دقیق دسترسی کاربران، امنیت عملیاتی را به شکل چشمگیری ارتقاء می‌دهد.

با رعایت این اصول و بهره‌گیری از راهکارهای حرفه‌ای امنیتی، می‌توان سطح امنیت داده‌ها و سامانه‌ها در دورکاری را به طور چشمگیری افزایش داد. شرکت مدیران شبکه برنا با بیش از ده سال تجربه در حوزه امنیت اطلاعات، خدماتی شامل آموزش، مشاوره، پیاده‌سازی و پشتیبانی راهکارهای امنیتی مانند Safetica ، ESET و PAM Arcon را ارائه می‌دهد تا سازمان‌ها و افراد بتوانند با اطمینان کامل به فعالیت‌های دورکاری خود ادامه دهند و در برابر تهدیدات سایبری مصون بمانند.

هشدار امنیتی جدی برای تیم‌های استفاده‌کننده از Telnet

آسیب‌پذیری بحرانی CVE-2026-24061 در GNU Inetutils

در ژانویه ۲۰۲۶ یک آسیب‌پذیری بسیار بحرانی با شناسه CVE-2026-24061 در سرویس telnetd از مجموعه GNU Inetutils شناسایی شد که امکان دور زدن کامل فرآیند احراز هویت از راه دور را برای مهاجمان فراهم می‌کند. این آسیب‌پذیری با امتیاز 9.8 از 10 (Critical) در CVSS v3.1 ارزیابی شده و به دلیل وجود شواهد سوءاستفاده فعال، به‌طور رسمی در فهرست Known Exploited Vulnerabilities سازمان CISA قرار گرفته است.

مشکل اصلی این آسیب‌پذیری به نحوه پردازش نادرست متغیر محیطی USER در نسخه‌های آسیب‌پذیر GNU Inetutils (از 1.9.3 تا 2.7) بازمی گردد. در این شرایط، مهاجم می‌تواند با تزریق آرگومان مخرب، احراز هویت را به‌طور کامل دور زده و بدون نیاز به نام کاربری یا رمز عبور، مستقیماً به سطح دسترسی root دست پیدا کند. این موضوع به‌ویژه برای زیرساخت‌هایی که هنوز به Telnet متکی هستند، یک تهدید بسیار جدی و فوری محسوب می‌شود.

خطر این آسیب‌پذیری تنها در تئوری خلاصه نمی‌شود. ماهیت حمله کاملاً از راه دور است، نیازی به دسترسی اولیه یا تعامل کاربر ندارد و می‌تواند منجر به تصرف کامل سیستم، تغییر تنظیمات حیاتی و ایجاد دسترسی پایدار برای مهاجم شود. به همین دلیل، استفاده از Telnet در چنین شرایطی عملاً به‌منزله باز گذاشتن درِ ورودی شبکه برای مهاجمان است.

سازمان‌ها و تیم‌های فنی که همچنان Telnet را در محیط عملیاتی خود فعال دارند، باید این آسیب پذیری را یک هشدار قرمز تلقی کنند. به‌روزرسانی سریع بسته‌های آسیب‌پذیر، غیرفعال‌سازی Telnet و مهاجرت به پروتکل‌های امن‌تر مانند SSH، حداقل اقداماتی است که باید در کوتاه‌ترین زمان ممکن انجام شود. هرگونه تأخیر در این مسیر، ریسک نفوذ و compromise کامل زیرساخت را به‌شدت افزایش می دهد.

برنا؛ همراه شما در مواجهه با تهدیدات بحرانی

شرکت برنا با تمرکز بر امنیت شبکه و مدیریت آسیب پذیری‌ها، به سازمان‌ها کمک می‌کند تا ریسک‌های ناشی از سرویس‌های قدیمی و ناامن مانند Telnet را شناسایی، تحلیل و برطرف کنند و در برابر تهدیدات فعال و بحرانی ایمن بمانند.

هشدار امنیتی درباره نشت گسترده اطلاعات کاربران اینستاگرام

افشای داده‌های ۱۷.۵ میلیون حساب کاربری و افزایش ریسک حملات فیشینگ

بر اساس گزارشی که به‌تازگی توسط شرکت امنیتی Malwarebytes منتشر شده، اطلاعات مربوط به حدود ۱۷.۵ میلیون حساب کاربری اینستاگرام در یک نشت گسترده داده افشا شده و هم‌اکنون به‌صورت آزاد در فروم‌های هکری و دارک‌وب در حال انتشار است. این موضوع میلیون ها کاربر و همچنین سازمان‌هایی که از اینستاگرام به‌عنوان بستر ارتباطی یا تجاری استفاده می کنند را در معرض ریسک مستقیم قرار داده است.

طبق اعلام Malwarebytes، این داده‌ها در جریان پایش‌های معمول دارک‌وب شناسایی شده و شامل اطلاعات حساسی مانند نام کاربری، نام و نام خانوادگی، آدرس ایمیل، شماره تلفن، بخش هایی از آدرس فیزیکی و سایر اطلاعات تماس است. هرچند شواهدی مبنی بر افشای مستقیم رمزهای عبور وجود ندارد، اما همین حجم از اطلاعات برای اجرای حملات هدفمند کاملاً کافی است.

www.bornanetwork.co info@bornanetwork.co ۰۲۱-۷۴۰۲۸

تحلیل‌ها نشان می‌دهد این نشت احتمالاً ریشه در یک API Leak در سال ۲۰۲۴ دارد. در تاریخ ۷ ژانویه، یک عامل تهدید با نام مستعار «Solonik» این دیتاست را در فروم BreachForums منتشر کرده و مدعی شده بیش از ۱۷ میلیون رکورد از کاربران اینستاگرام را در قالب فایل های JSON و TXT در اختیار دارد. ساختار داده‌های افشاشده شباهت زیادی به پاسخ‌های API دارد و این موضوع فرضیه‌هایی مانند scraping گسترده، endpoint ناامن یا پیکربندی نادرست سیستم‌ها را تقویت می کند. با این حال، منبع دقیق نشت هنوز به‌طور رسمی تأیید نشده است.

شرکت Meta، مالک اینستاگرام، تا زمان انتشار این گزارش واکنش رسمی یا تأییدی نسبت به این رخداد ارائه نکرده است. در همین حال، گزارش‌های متعددی از سوی کاربران منتشر شده که نشان می‌دهد پس از افشای این داده‌ها، ایمیل‌های غیرمنتظره‌ای با موضوع بازیابی رمز عبور اینستاگرام دریافت کرده‌اند. Malwarebytes هشدار داده است که بخشی از این ایمیل‌ها ممکن است واقعی و بخشی دیگر بخشی از حملات فیشینگ و سوءاستفاده از مکانیزم بازیابی حساب باشند.

.

خطر اصلی این نشت داده، امکان اجرای حملاتی مانند فیشینگ هدفمند، جعل هویت، سوءاستفاده از فرآیند بازیابی حساب، SIM Swapping و جمع آوری اعتبارنامه‌ها است. در محیط‌های سازمانی، این موضوع می‌تواند به تصاحب حساب‌های رسمی، انتشار محتوای مخرب، آسیب به اعتبار برند و حتی نفوذ به سایر سامانه‌ها از طریق مهندسی اجتماعی منجر شود.

این رخداد بار دیگر نشان می‌دهد که حتی بدون افشای رمز عبور، نشت اطلاعات تماس می تواند زمینه‌ساز حملات گسترده و زنجیره‌ای باشد. کاربران و تیم‌های امنیتی باید نسبت به ایمیل ها و پیام‌های مشکوک هوشیار باشند و هرگونه پیام بازیابی حساب که بدون درخواست دریافت شده است را به‌عنوان یک هشدار جدی در نظر بگیرند.

برنا؛ همراه شما در مدیریت ریسک نشت داده و تهدیدات سایبری

شرکت برنا با ارائه راهکارهای امنیتی پیشرفته، به سازمان‌ها کمک می‌کند تا ریسک‌های ناشی از نشت اطلاعات، فیشینگ و سوءاستفاده از حساب‌های کاربری را شناسایی و کنترل کنند. پایش دارک‌وب، مدیریت رخدادهای امنیتی و افزایش آگاهی کاربران، بخشی از خدمات برنا برای مقابله با چنین تهدیداتی است.

سخن پایانی

شرکت « مدیران شبکه برنا » با پشتوانه ای از تجربه و دانش تخصصی و تمرکز بر ارائه راهکارهای نوین امنیت شبکه همواره تلاش کرده است تا نیازهای امنیتی سازمان ها و شرکت ها را در بالاترین سطح پوشش دهد . ما با بهره گیری از محصولات و فناوری های برتر جهانی در حوزه های چون , DLP EDR , XDR فایروال ؛ انتی ویروس DRM و NDR سعی کرده ایم فضای سایبری امن و پایدار برای مشتریان خود فراهم کنیم.
ماموریت ما فراتر از ارائه محصول است . ما به دنبال ارائه راهکارهایی هستیم که نه تنها امنیت شبکه و داده های سازمان ها را تضمین می کنند بلکه امکان مدیریت هوشمند تهدیدات ؛ انطباق پذیری با الزامات قانونی و افزایش بهره وری فناوری اطلاعات را نیز به همراه دارند . در این مسیر ؛ تیم فنی متخصص ؛ پشتیبانی سریع و ارائه مشاوره دقیق ؛ از ارزش های محوری شرکت ما به شمار می آیند.
ما باور داریم که امنیت سایبری صرفا یک محصول نیست ؛ بلکه یک تعهد دائمی و یک رویکرد حرفه ای برای حفظ سرمایه های اطلاعاتی سازمان هاست.شرکت مدیران شبکه برنا همواره همراهی قابل اعتماد برای سازمان ها و مدیران فناوری اطلاعات بوده و خواهد بود.

در پایان ؛ امیدواریم این رزومه بتواند نمایی شفاف از توانمندی ها ؛ حوزه های تخصصی و خدمات ما ارائه دهد و زمینه ساز همکاری های حرفه ای و مؤثر با سازمان شما باشد . آماده ایم تا در کنار شما ؛ گامی مطمئن در مسیر توسعه و امنیت برداریم.

www.bornanetwork.co info@bornanetwork.co ۰۲۱-۷۴۰۲۸