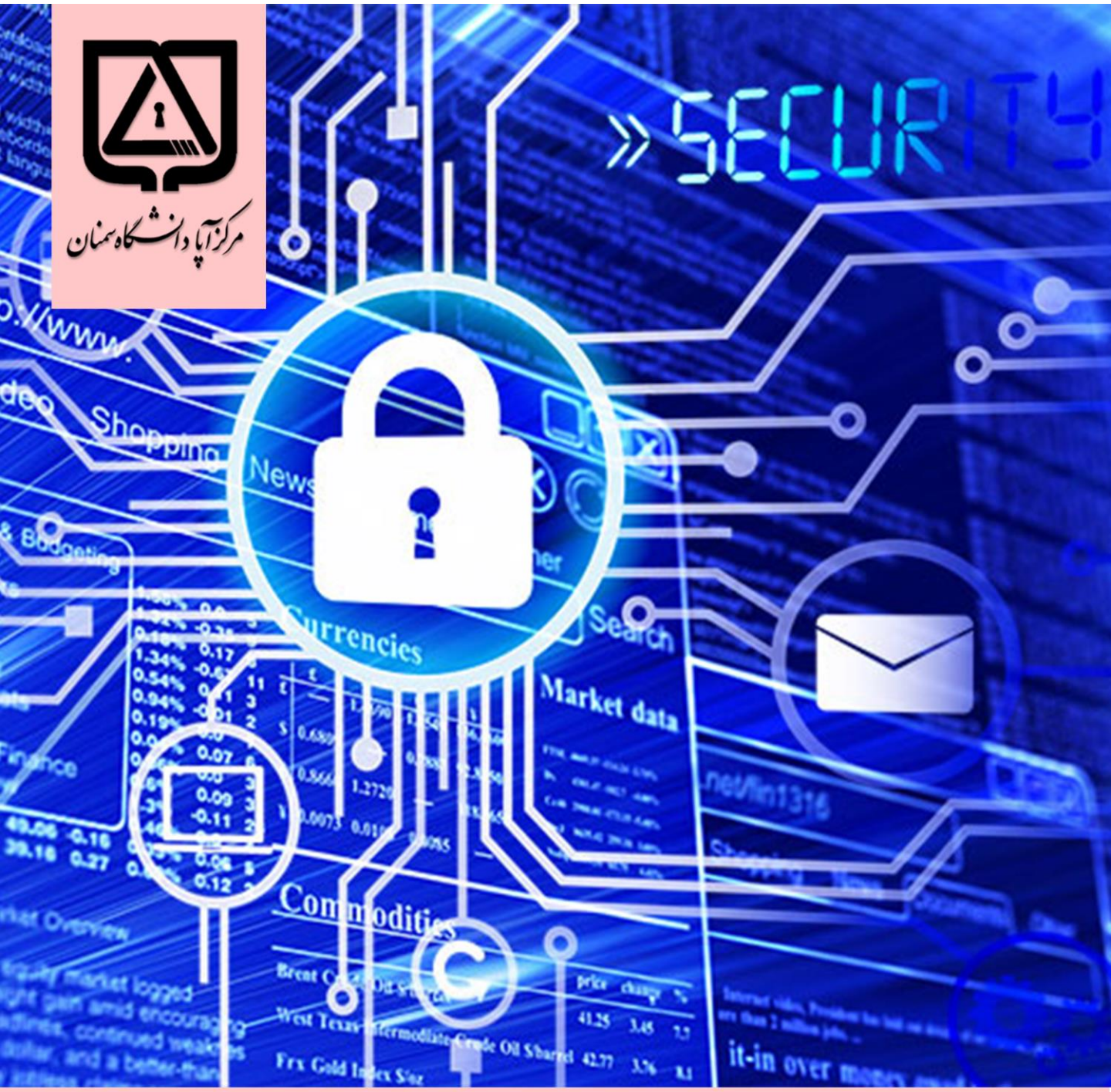

خبرنامه الکترونیکی ۷۵

مرکز تخصصی آپا دانشگاه سمنان

در این شماره می‌خوانید:

امنیت هوشمندانه در سازمان (بخش اول)

شماره هفتاد و پنجم، سال نهم، فروردین ۱۴۰۵ |کاری از تیم تولید محتوای مرکز تخصصی آپای دانشگاه سمنان

https://cert.semnan.ac.ir info.cert@semnan.ac.ir ۰۲۳-۳۱۵۳۵۰۲۱ @semcert

فهرست

خبر

کشف آسیب‌پذیری‌های دسترسی مدیریتی از طریق نام‌کاربری و رمز پیش‌فرض در فریمور SODOLA SL۹۰۲-SWTGW۱۲۴AS ۴

کشف آسیب پذیری در Fortinet FortiClient EMS ۵

امنیت هوشمندانه در سازمان (بخش اول) ۷

مرکز آپا دانشگاه سمنان

اخبار امنیت سایبری

SODOLA
POE NETWORKS

کشف آسیب‌پذیری‌های دسترسی مدیریتی از طریق نام‌کاربری و رمز پیش‌فرض در فریمور SODOLA SL۹۰۲-SWTGW۱۲۴AS

آسیب‌پذیری CVE-۲۰۲۶-۲۷۷۵۱ در فریمور SODOLA SL۹۰۲-SWTGW۱۲۴AS با شدت ۹.۸ به دلیل استفاده از نام‌کاربری و رمز عبور پیش‌فرض در رابط مدیریتی رخ می‌دهد. مهاجم از راه دور می‌تواند بدون نیاز به تغییر رمز، به پنل مدیریت دسترسی پیدا کرده و کنترل کامل دستگاه را به دست بگیرد. این دسترسی شامل تغییر پیکربندی شبکه، تنظیمات امنیتی و دیگر تنظیمات حیاتی دستگاه است. بهره‌برداری از این آسیب‌پذیری ساده و تنها مستلزم دسترسی شبکه‌ای به دستگاه است. عدم اصلاح این مشکل می‌تواند منجر به نفوذ به شبکه‌های داخلی یا حتی کنترل دستگاه از طریق اینترنت شود. برای کاهش ریسک، تغییر فوری اعتبارنامه پیش‌فرض به یک رمز عبور قوی ضروری است. علاوه بر این، محدودسازی دسترسی به رابط مدیریتی، فعال‌سازی لاگ‌برداری و مانیتورینگ فعالیت‌ها توصیه می‌شود تا سوءاستفاده احتمالی شناسایی و جلوگیری شود.

محصولات تحت تاثیر:

SODOLA SL۹۰۲-SWTGW۱۲۴AS

- تجهیزات شبکه/سوییچ با رابط مدیریتی تحت فریمور آسیب‌پذیر

نسخه‌های آسیب‌پذیر: تا ۲۰۰.۱.۲۰

استقرارهایی که دستگاه‌ها در شبکه‌های داخلی یا در دسترس شبکه عمومی قرار دارند

توصیه های امنیتی:

تغییر فوری نام‌کاربری و رمز عبور پیش‌فرض به مقادیر قوی و پیچیده

محدود کردن دسترسی به رابط مدیریتی فقط به IPهای مجاز یا شبکه داخلی

غیرفعال‌سازی دسترسی مدیریتی از اینترنت در صورت امکان

فعال‌سازی لاگ‌برداری و مانیتورینگ فعالیت‌های مدیریتی

اعمال اصل حداقل سطح دسترسی (Least Privilege) برای کاربران و سرویس‌ها

به‌روزرسانی Firmware به نسخه‌ای که این آسیب‌پذیری اصلاح شده است

بررسی حساب‌های مدیریتی موجود و حذف یا محدودسازی هر حساب غیرضروری

کشف آسیب پذیری در Fortinet FortiClient EMS

آسیب‌پذیری بحرانی در Fortinet FortiClient EMS برای مدیریت endpointها کشف شده است. این ضعف با شناسه CVE-۲۰۲۶-۳۵۶۱۶ و امتیاز Critical) CVSS: ۹.۸) شناسایی شده و در حال حاضر به‌صورت گسترده در حملات واقعی مورد بهره‌برداری قرار می‌گیرد. این آسیب‌پذیری به مهاجم غیرمجاز اجازه می‌دهد کنترل سیستم مدیریت endpoint را به دست بگیرد. شدت این آسیب‌پذیری بالا (HIGH) ارزیابی شده است. مهاجم ابتدا به سیستم Enterprise Management Server) EMS) دسترسی پیدا می‌کند و سپس exploit را اجرا می‌کند. در نتیجه، تمام endpointهای متصل به این سیستم مدیریتی compromise می‌شوند. از آنجا که EMS نقش مدیریتی دارد، compromise شدن آن به معنای کنترل چندین سیستم تحت مدیریت است.

محصولات تحت تاثیر:

FortiClient EMS ۷.۴.۵ تا ۷.۴.۶.

توصیه های امنیتی:

اقدام فوری: Patch امنیتی را در اسرع وقت اعمال کنید.

دسترسی به سیستم EMS را محدود و کنترل‌شده کنید.

لاگ‌ها و رفتار endpointهای متصل را به‌صورت مداوم مانیتور کنید.

از قرار دادن EMS در معرض اینترنت خودداری کنید.

مرکز آپا دانشگاه سمنان

امنیت هوشمندانه در سازمان

امنیت هوشمندانه در سازمان (بخش اول)

مقدمه‌ای برای کارمندان: چرا امنیت دیگر «انتخاب» نیست؟

در سال‌های اخیر، امنیت اطلاعات از یک موضوع فنی و محدود، به یکی از مهم‌ترین دغدغه‌های سازمان های دولتی، دانشگاهی و خصوصی تبدیل شده است. حملاتی که روزی تنها شبکه‌های بزرگ جهانی را تهدید می‌کردند، امروز می‌توانند یک اداره کوچک، یک شرکت خدماتی و حتی حساب شخصی یک کارمند را هدف بگیرند.

نکته مهم این است که **امنیت دیگر فقط یک وظیفه فنی نیست؛ بلکه ترکیبی از فناوری، رفتار کارکنان و مدیریت هوشمندانه است.**

این یعنی هر کارمند، بدون نیاز به دانش تخصصی، نقشی اساسی در امنیت یا ناامنی سازمان ایفا می کند.

این مجموعه با هدف معرفی اصول «امنیت هوشمندانه» طراحی شده است؛ اصولی که ساده، عملی و قابل اجرا در محیط‌های اداری هستند. در این شماره، پایه‌ای‌ترین مفاهیم را مرور می‌کنیم.

۱. امنیت هوشمندانه یعنی چه؟

امنیت هوشمندانه به رویکردی گفته می‌شود که در آن سازمان:

- **تهدیدها را پیش‌بینی** می‌کند،
- **رفتار کاربران را تحلیل** می‌کند،
- **راهکارهای مناسب را متناسب با نیاز** خود انتخاب می‌کند،
- و از **نقش کلیدی کارمندان** در تضمین امنیت غافل نمی‌شود.

به زبان ساده‌تر:

به‌جای اینکه فقط «در را قفل کنیم»، باید بدانیم **چه کسی وارد می‌شود، چرا وارد می‌شود، و چه اتفاقی ممکن است بیفتد.**

امنیت هوشمندانه در سازمان (بخش اول)

۲. چرا کارمندان مهم‌ترین حلقه امنیت هستند؟

بیش از ۷۰ درصد حوادث امنیتی سازمانی (براساس آمار جهانی) به دلیل سهو، ناآگاهی یا اشتباه کارکنان رخ می‌دهد؛ نه نقص فنی.

چند مثال واقعی (البته بدون جزئیات سازمانی):

- کارمندی که ایمیل جعلی «آپدیت حقوق» را باز کرد و رمز سامانه‌اش سرقت شد.
- کارشناس اداری که فلش ناشناس را به سیستم وصل کرد و شبکه آلوده شد.
- کاربری که رمز عبور خود را روی یک برگه کنار مانیتور چسبانده بود.
- عضوی از مجموعه که فایل محرمانه را اشتباهی به گروه واتساپی خانوادگی ارسال کرد.

این حوادث، با رعایت چند رفتار ساده قابل جلوگیری بودند.

بنابراین کارمند آموزش‌دیده بزرگ‌ترین دارایی امنیتی سازمان است.

۳. سه ستون اصلی امنیت هوشمندانه برای کارمندان

مطالب این سری بر پایه سه اصل طراحی می‌شود:

۱) آگاهی

شناخت تهدیدات روزمره:

ایمیل‌های جعلی، لینک‌های مشکوک، پیام‌های فریبنده، برنامه‌های ناشناس، تماس‌های ساختگی و...

۲) رفتار

چگونه با سامانه‌ها، فایل‌ها و داده‌ها تعامل کنیم که کمترین خطر را داشته باشد.

مثلاً:

- رمز قوی
- استفاده صحیح از اینترنت سازمان
- مراقبت از دستگاه‌های کاری
- تشخیص درخواست‌های مشکوک

۳) همکاری

هیچ فردی به‌تنهایی امنیت را حفظ نمی‌کند.

گزارش سریع خطاها یا موارد مشکوک به واحد فناوری، حتی اگر «مسخره» یا «کوچک» به نظر برسد، بسیار مهم است.

در این شماره بیشتر بر **آگاهی** تمرکز می‌کنیم.

۴. تهدیدات روزمره‌ای که یک کارمند باید بشناسد

در ادامه، ۵ تهدید رایج که تقریباً در تمام سازمان‌ها مشاهده می‌شوند را معرفی می‌کنیم.

۴-۱. ایمیل‌ها و پیام‌های فیشینگ

فیشینگ یعنی تلاش مهاجم برای فریب شما تا اطلاعات حساس را بدهید یا فایل آلوده را باز کنید.

نشانه‌های رایج یک پیام مشکوک:

- فوریت غیرعادی: «همین الان باز کن»، «حساب شما مسدود می‌شود»
- غلط‌های نگارشی
- درخواست اطلاعات محرمانه
- لینک‌هایی که با متن واقعی یکی نیستند
- ضمیمه‌هایی با فرمت‌های ناشناس

اصل طلایی:

اگر ۱ درصد شک دارید، باز نکنید و با واحد IT تماس بگیرید.

۴-۲. مهندسی اجتماعی

هکرها لزوماً پشت کامپیوتر نیستند؛

گاهی پشت تلفن‌اند و به‌عنوان «پشتیبانی سامانه»، «کارمند جدید»، یا «بازرس» معرفی می‌شوند.

اگر کسی تلفنی، پیامکی یا حضوری درخواست اطلاعات امنیتی کرد:

- رمز عبور را هرگز به کسی اعلام نکنید.
- قبل از همکاری، هویت فرد را از طریق واحدهای داخلی تأیید کنید.

۴-۳. حافظه‌های USB و ابزارهای ناشناس

یک فلش کوچک می‌تواند کل شبکه را آلوده کند.

اگر فلشی روی میز پیدا کردید یا شخصی بیرونی داد:

- زیر هیچ شرایطی مستقیم به سیستم وصل نکنید.
- آن را برای بررسی به واحد IT تحویل دهید.

۴-۴. استفاده از شبکه‌های اجتماعی در محیط کار

اشتراک یک عکس از میز کار می‌تواند اطلاعاتی مثل:

لیست جلسات، نام سامانه‌ها یا حتی کدهای داخلی را لو بدهد.

مراقب باشید چه چیزی و از کجا منتشر می‌کنید.

۴-۵. رمزهای عبور ضعیف

هنوز هم رایج‌ترین رمزهای کاربران:

۱۲۳۴۵۶
password
۱۱۱۱۱۱

تاریخ تولد
شماره تلفن
رمز قوی یعنی ترکیبی از:
حروف بزرگ، کوچک، عدد و علامت، با طول حداقل ۱۰ کاراکتر.

۵. چگونه امنیت را به یک عادت تبدیل کنیم؟

رفتارهای کوچک، تأثیر بزرگ دارند.

پیشنهاد می‌شود کارمندان این ۶ عادت را از همین امروز اجرا کنند:

- قبل از باز کردن لینک‌ها، یک ثانیه مکث کنید.
- رمزهای تکراری در چند سامانه نگذارید.
- هر مورد مشکوک را سریع گزارش کنید.
- در محیط عمومی درباره سیستم‌ها و مشکلاتشان صحبت نکنید.
- دستگاه کاری را بدون رمز رها نکنید.
- فایل‌ها و اطلاعات را فقط از منابع رسمی دریافت کنید.

۶. جمع‌بندی: گام اول در امنیت هوشمندانه

در این شماره یاد گرفتیم که امنیت هوشمندانه از رفتار کارکنان شروع می‌شود.
شناخت تهدیدات روزمره، اولین قدم است.
در شماره‌های بعدی، وارد موضوعات کاربردی‌تر می‌شویم از جمله:

- مدیریت رمزها و احراز هویت چندمرحله‌ای
- تشخیص پیام‌های جعلی
- نحوه کار ایمن با سیستم‌های سازمانی
- امنیت موبایل و لپ‌تاپ کاری
- و خطاهای رایج امنیتی کارکنان

ما را در تلگرام دنبال کنید :

@semcert