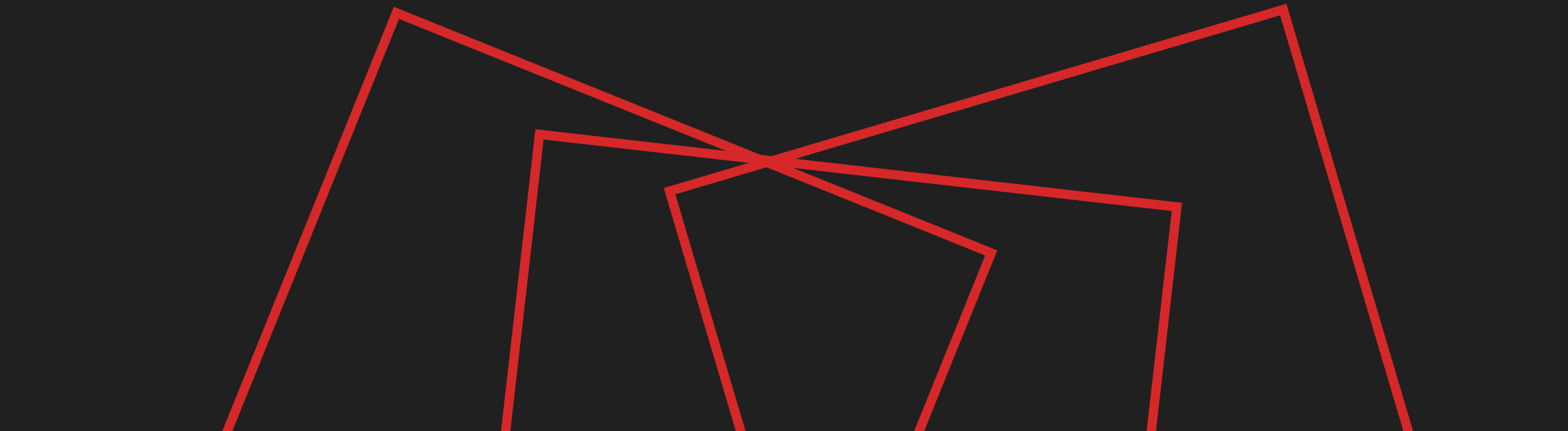
# راهنمای کاربردی شناخت، مواجهه و مدیریت رخدادهای سایبری

گزارش اول- بهار ۱۴۰۵

انجمن تجارت الکترونیک تهران
TEHRAN



# برای حادثه‌هایی نزدیک‌تر از آن‌چه به‌نظر می‌رسند، چه باید کرد؟

وقتی پازل رخدادهای سیاسی، اقتصادی و اجتماعی سال ۱۴۰۴ و تمام آسیب‌هایی که کسب‌وکارهای اقتصاد دیجیتال در زمان قطعی اینترنت را کنار هم می‌گذاریم نباید از یک مولفه‌ی مهم غافل شد؛ **امنیت سایبری! چیزی که به بهانه‌ی حفظ آن، اینترنت در سال گذشته نزدیک به ۵۷ روز قطع شد. این درحالی‌ست که بررسی و نظر تخصصی کارشناسان حوزه‌ی امنیت نشان می‌دهد که سیاست محدودسازی اینترنت نمی‌تواند مانعی برای اتفاق یا شدت حمله‌های سایبری به کسب‌وکارها باشد؛مشابه آن‌چه در جریان حمله‌ی اسراییل در جنگ ۱۲روزه رخ داد. فارغ از این‌که همواره ما در انجمن تجارت الکترونیک تهران، مطالبه‌ی اینترنت آزاد برای همه‌ی مردم ایران را خواستاریم، در این گزارش می‌خواهیم روی آمادگی امنیتی و فنی کسب‌وکارها و دانش مدیران ارشد فنی کسب‌وکارها تاکید کنیم. بررسی‌های ما نشان می‌دهد که در کسب‌وکارهای آنلاین کشور نوعی خلا اطلاعاتی نسبت به اقدام‌های پیش‌گیرانه و راهکارهای فوری مدیریت بحران، تاب‌آوری سازمان‌ها وجود دارد. این گزارش با هدف افزایش آمادگی و مدیریت بحران‌های امنیتی تدوین شده است تا** در روز وقوع حمله، میزان خطر و خسارت به کم‌ترین حالت ممکن برسد. به همین دلیل تلاش شده است تا با توجه به تنوع معماری و زیرساخت در کسب‌وکارهای مختلف کشور، راهکارهای ارایه‌شده به‌گونه‌ای تنظیم شود که بیشترین اثربخشی را برای طیف وسیعی از سازمان‌ها داشته باشند.

این گزارش در سه بخش

۱. **آشنایی با تهدیدهای سایبری**

۲. **اقدام‌های ضروری پیش از مواجهه با بحران سایبری**

۳. **راهکارهای مدیریتی در هنگام مواجهه با بحران سایبری** نوشته شده است.

روش پژوهش و گردآوری این گزارش براساس مشاهدات پرتکرار و تجارب عملی متخصصان جرم‌یابی دیجیتال و کارشناسان امنیت سایبری کشور است؛ به همین دلیل این گزارش می‌تواند راهنمای کاربردی و تجربه‌محور برای عبور از بحران‌های سایبری باشد و از مخاطب‌های این گزارش دعوت می‌کنیم که درصورت داشتن نکات تکمیلی، در تداوم تهیه و انتشار چنین گزارش‌هایی همراهی کنند.

# ۰۱

# تصویری از بحران امنیت سایبری؛

## از نفوذهای سطحی تا تهدیداتی پایدار

# تصویری از بحران امنیت سایبری؛

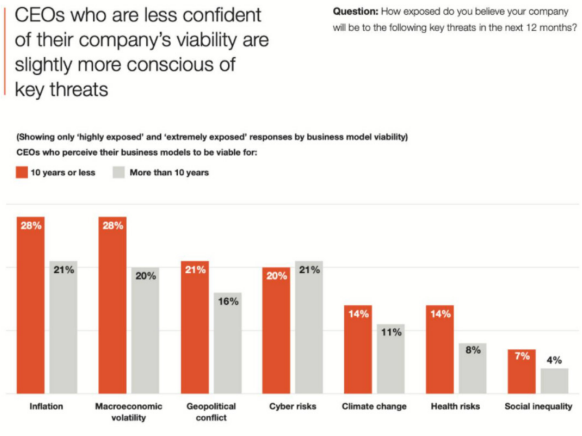
## از نفوذهای سطحی تا تهدیداتی پایدار

در گزارش موسسه **PwC** مربوط به سال ۲۰۲۵، ریسک‌های سایبری در کنار درگیری‌های ژئوپلیتیک به یکی از مهم‌ترین تهدیدهای پیش‌روی مدیران عامل در جهان تبدیل شده‌اند و مدیران عامل آن را تهدیدی بلندمدت، دایمی و ساختاری معرفی کردند.

تنوع قربانیان رخدادهای سایبری نشان می‌دهد که امروزه هیچ سازمانی، صرف‌نظر از اندازه یا حوزه فعالیت، خارج از دایره تهدید حملات سایبری قرار ندارد. بررسی آسیب‌پذیری‌های منتشرشده توسط NIST[1]، حاکی از این است که سالانه بین ۲۵ تا ۳۰ هزار آسیب‌پذیری امنیتی جدید در نرم‌افزارها و سامانه‌ها کشف و ثبت می‌شود. در کنار افزایش سالیانه‌ی تعداد اسیب‌پذیری‌ها، نکته‌ی نگران‌کننده‌ی ماجرا آن جاست که در فضای دارک‌وب، تنها با پرداخت چند دلار می‌توان دسترسی به سیستم‌های آلوده و زیرساخت‌های در معرض نفوذ را خریداری کرد.

ورود ابزارهای هوش مصنوعی، به‌ویژه مدل‌های مولد، سرعت، مقیاس و دقت حملات سایبری را به‌طور چشمگیری افزایش داده است؛ از تولید مداوم حملات فیشینگ که به‌طور کامل شخصی‌سازی شده‌اند تا کشف سریع‌تر آسیب‌پذیری‌ها و خودکارسازی مراحل نفوذ را شامل می‌شود. در نتیجه، مهاجمان امروز می‌توانند حملاتی را اجرا کنند که پیش‌تر فقط در توان گروه‌های بسیار حرفه‌ای بود.

نکته‌ی قابل‌تامل دیگر آن است که بررسی قربانیان حملات سایبری هدفمند پیچیده (APT)، نشان می‌دهد مهاجمان از ۱۰ روز تا بیش از یک سال پیش از اجرای حمله اصلی، به‌شکل پنهان در شبکه قربانیان حضور داشته‌اند و رفتار سازمان را رصد می‌کنند. درنهایت خبر بد این است که مهاجمان همیشه چند گام جلوتر از لایه‌های دفاعی سازمان حرکت می‌کنند آنها با شناخت دقیق زیرساخت، الگوهای رفتاری کاربران و نقاط ضعف فرآیندی یا فنی، حمله نهایی خود را در زمانی اجرا می‌کنند که سازمان کمترین آمادگی را برای شناسایی یا مقابله دارد.




PwC's 27th Annual Global CEO Survey مربوط به سال ۲۰۲۵،

۱. National Vulnerability Database

# آشنایی با انواع تهدیدات سایبری

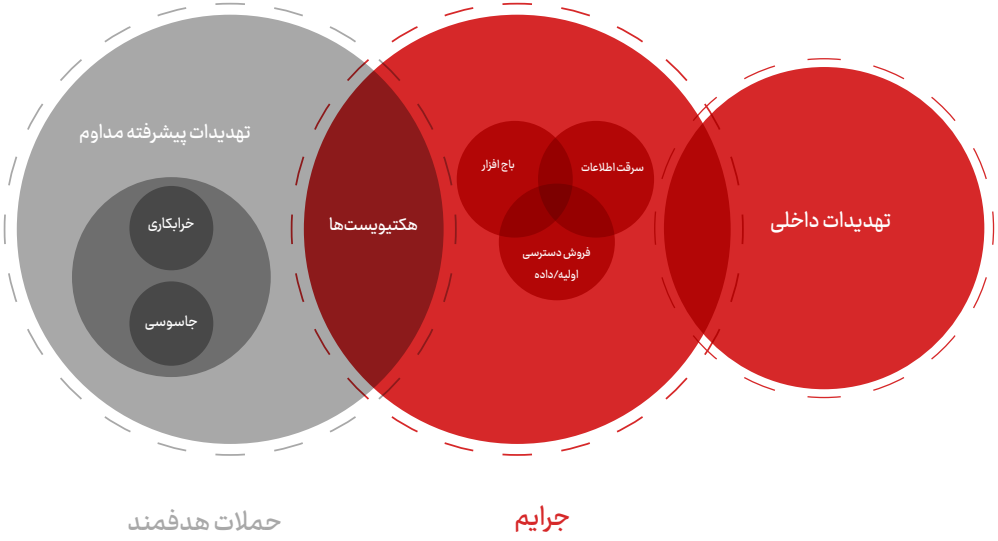
شناخت انگیزه‌ها و الگوهای رفتاری گروه‌های هکری به سازمان‌ها کمک می‌کند تا درک بهتری از ماهیت تهدیدات سایبری داشته باشند و بر اساس آن، راهبردهای دفاعی مؤثرتر و واکنش‌های مناسب‌تری طراحی کنند. بر همین اساس، تهدیدات سایبری را می‌توان بر پایه انگیزه و ماهیت حمله در چهار دسته اصلی طبقه‌بندی کرد.

۱ جرایم سایبری با انگیزه‌های مالی یا کسب اعتبار

۲ حملات گروه‌های هکتیویستی
Hacktivism

۳ حملات هدفمند و پیشرفته
Advanced Persistent Threat (APT)

۴ تهدیدات داخلی
Insider Threat



# ۱ جرایم سایبری با انگیزه‌ی مالی یا کسب اعتبار

این دسته از حمله‌ها، شامل فعالیت‌های هکر/گروه‌های هکری می‌شود که هدف اصلی آن کسب درآمد، یا کسب شهرت از روش‌های مجرمانه است.

## سرقت اطلاعات

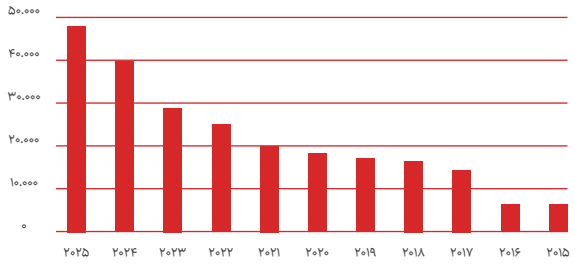
در این حملات تمرکز نفوذگران بیشتر ابر سرقت اطلاعات مالی (مانند اطلاعات کارت بانکی و حساب‌های کاربری)، سرقت هویت دیجیتال، برداشت غیرمجاز از داده‌های سازمانی، سرقت کوکی‌ها، نشست‌ها (Session) و رمزهای عبور است. تهدید به انتشار داده‌ها به‌شکل عمومی با هدف لطمه زدن به اعتبار کسب‌وکار، یا درخواست دریافت پول به ازای افشانشدن اطلاعات، از شگردهای این گروه از نفوذگران است.

### روش نفوذ رایج

نفوذگران با بهره‌گیری از آسیب‌پذیری‌های شناخته‌شده (CVE، CWE) در سطح سرویس‌ها و کتابخانه‌ها، یا سواستفاده از آسیب‌پذیری‌های منطقی، اقدام به سرقت اطلاعات می‌کنند.

### اقدام‌های پیش‌گیرانه

**پیاده‌سازی چرخه‌ی کامل مدیریت آسیب‌پذیری (Vulnerability Management) و انجام تست نفوذ مستمر**




تعداد رکوردهای CVEهای ثبت شده به تفکیک سال

# باج‌افزار

رمزگذاری غیرقابل‌بازگشت داده‌ها و درخواست باج برای ارایه‌ی کلید رمزگشایی، تهدید به افشا یا تخریب اطلاعات، حمله به زنجیره‌ی تامین برای ایجاد خسارتی گسترده‌تر، از روش‌های رایج این نوع حملات هستند.

در برخی سازمان‌ها، به‌دلیل حجم بالای داده‌ها یا ماهیت تخصصی آن‌ها، دسترسی مستقیم به محتوای داده برای گروه‌های هکری اهمیت چندانی ندارد. در چنین مواردی، مهاجمان معمولاً با استفاده از باج‌افزار، اقدام به اخاذی از کسب‌وکار می‌کنند. کسب‌وکارهایی که حیات آن‌ها به داده‌های دیجیتال وابسته است، اهداف بسیار جذابی برای این دسته از نفوذگران به شمار می‌روند.

در این حملات نفوذگر پس از به‌دست آوردن دسترسی اولیه با حفظ و افزایش سطح دسترسی، ساختار ارتباط سازمان و الگوهای تهیه‌ی نسخه‌ی پشتیبان را زیر نظر می‌گیرند تا در یک حمله‌ی زمان‌بندی‌شده، تجهیزات زیرساختی و سامانه‌های پشتیبان را هم‌زمان آلوده کرده و بیش‌ترین میزان آسیب را به سازمان وارد کنند.

## ۷۸ درصد سازمان‌ها در خطر باج‌افزارها!

CrowdStrikeدر یک نظرسنجی جهانی که از ۱۱۰۰ مدیر امنیت سایبری (CIO, CISO, SecOps) انجام داده،نشان می‌دهد:

٪۷۸ سازمان‌ها در ۱۲ ماه گذشته هدف باج‌افزار قرار گرفته‌اند

این عدد در سال ۲۰۲۴ حدود ٪۶۶ بود. یعنی افزایش تقریباً ۱۲ درصدی نرخ حملات در یک سال!

## روش نفوذ رایج

مشاهده‌ی متخصصان نشان می‌دهد که نفوذگران با بهره‌گیری از ابزارهای خودکار، حمله را به‌شکل گسترده و غیرهدفمند آغاز می‌کنند تا دسترسی اولیه‌ای بدست بیاورند. هم‌چنین در مواردی هم دسترس اولیه از راه ارسال ایمیل با محتوای آلوده و اجرای فایل مخرب از سوی کاربر نهایی مشاهده شده است.

## اقدام‌های پیش‌گیرانه

**استفاده از نسخه‌های پشتیبان آفلاین و غیرقابل‌تغییر (Immutable Offline Backups)**

این مهم‌ترین سد دفاعی در برابر باج‌افزار است؛ زیرا حتی در حالت رمزگذاری کامل داده‌ها، سازمان می‌تواند بدون پرداخت باج، سرویس‌ها را بازیابی کند.

## توصیه امنیتی: در مواجهه با حملات باج‌افزاری، به هیچ وجه باج پرداخت نکنید.

پرداخت باج باعث افزایش انگیزه‌ی مهاجمان و تکرار حمله با درخواست مبلغ بیشتر خواهد شد بر اساس گزارش «CrowdStrike State of Ransomware Survey 2025»، پرداخت باج تضمینی برای حفظ داده‌ها نیست؛ در میان سازمان‌هایی که باج پرداخت کرده‌اند، **۹۳ درصد** اعلام کرده‌اند که **با وجود پرداخت، داده‌هایشان توسط مهاجمان به سرقت رفته است.**

**پرداخت باج یک راه حل نیست یک چرخه است.**

در برخی موارد، گروه‌های باج‌افزاری پس از شناسایی یا پایان فعالیت خود، کلیدهای رمزگشایی را به‌شکل عمومی منتشر می‌کنند. در حالتی که از باج‌افزارهای شناخته‌شده آسیب دیده‌اید و داده‌ی حیاتی از دست داده‌اید، توصیه می‌شود نسخه‌ی رمزشده‌ی اطلاعات را نگه دارید تا در آینده بتوان در حالت انتشار کلیدها، داده‌ها را بازیابی کنید.

# فروش دسترسی اولیه

بررسی‌ها نشان می‌دهد که در این نوع حملات، رفتار تخریبی یا اثری از نفوذ مشاهده نمی‌شود. نفوذگر با استفاده از ابزارهای خودکار از قربانیان دسترسی‌هایی را جمع‌آوری می‌کند و در آینده با فروش این دسترسی‌ها، کسب درآمد می‌کند. دسترسی‌ها به سیستم‌های آلوده در سازمان، RDPهای[۲] دسترسی دسکتاپ از راه دور آسیب‌پذیر، یا حساب‌های VPN و سایر حساب‌های کاربری افشا شده، معمولا در بازارهای زیرزمینی به‌عنوان نقطه ورود آماده برای حملات بعدی عرضه می‌شوند. گروه‌های هکری APT، مشتریان عمده‌ی خرید این‌گونه دسترسی‌ها در دارک وب هستند. با توجه به اینکه هدف نفوذگر در این حملات صرفا جمع‌آوری و فروش دسترسی است، احتمال شناسایی این حملات در زمان حادثه، پایین است.

## روش نفوذ رایج

مهاجمان معمولا با سواستفاده از عدم بروزرسانی، پیاده سازی ناامن سرویس‌های دسترسی راه دور مانندSSH, RDP یا VPN، استفاده از **گذرواژه‌های ضعیف یا افشاشده، نبود احراز هویت چندمرحله‌ای و ضعف در تنظیمات امنیتی تجهیزات لبه شبکه**، به زیرساخت سازمان دسترسی پیدا می‌کنند.

## اقدام‌های پیش‌گیرانه

**استقرار سامانه‌های مانیتورینگ + سامانه‌های PAM**[۳] همچنین استفاده از EDR می‌تواند رفتارهای مخرب و Backdoorهای مخفی ایجادشده از سوی نفوذگران را شناسایی و مسدود کند.

۳. Privileged Access Management

# فروش داده

فروش پایگاه‌داده‌های لورفته، شامل اطلاعات هویتی، ایمیل‌ها، رمزهای عبور و داده‌های مالی، یکی از رایج‌ترین شیوه‌های کسب درآمد برای مهاجمان است. در این نوع حملات، اندازه یا نوع کسب‌وکار اهمیت چندانی ندارد؛ زیرا هر میزان داده‌ی جمع‌آوری‌شده می‌تواند در آینده برای هکر ارزش مالی ایجاد کند.

کسب‌وکارهای نوپا و محصولاتی که بدون انجام ارزیابی امنیتی عرضه می‌شوند، در برابر این تهدیدات بسیار آسیب‌پذیر هستند. به‌علاوه، تجهیزات و سیستم‌های شخصی یا کاری کارمندان مانند، لپ‌تاپ‌ها، دستگاه‌های موبایل، به‌ویژه توسعه‌دهندگان نرم‌افزار سازمان، به‌دلیل نصب نرم‌افزارهای نامعتبر، آلوده شوند و داده‌های آن‌ها توسط نفوذگران جمع‌آوری شود. اهمیت این مساله تا آن‌جاست که در دارک‌وب، خدماتی با Data-As-a-Service ایجاد شده است که فقط با پرداخت چند دلار می‌توان به داده‌های افشا شده بر اساس نام شخص، دامنه یا سازمان دسترسی پیدا کرد؛ موضوعی که به مهاجمان برای یافتن مسیرهای جدید نفوذ به سازمان کمک می‌کند.

بر اساس گزارش IOCTA 2025 بزرگ‌ترین سهم از بازار خرید و فروش داده‌ها در دارک‌وب مربوط به **اطلاعات مالی و حساب‌های کاربری دیجیتال** است. هم‌زمان، تقاضا برای Data-as-a-Service در دارک‌وب با گسترش مدل‌های اشتراکی فروش داده، رشد چشمگیری را تجربه کرده است.[۶]

## روش نفوذ رایج

مهاجمان معمولا از راه سرقت یا حدس‌زدن اطلاعات هویتی کاربران (Credential Theft)، سواستفاده از حساب‌های با دسترسی بالا، بهره‌برداری از آسیب‌پذیری سرویس‌های دیتابیس یا وب‌سرورها، در پوشش نرم‌افزارهای رایگان، توسعه‌ی پلاگین‌های ناامن مرورگرها یا آلوده سازی منابع متن‌باز و بازنشر آنها وارد سیستم قربانیان می‌شوند و داده‌های حساس را استخراج می‌کنند.

## اقدام‌های پیش‌گیرانه

**جلوگیری از نشت داده** DLP[۴] مسیرهای خروج داده را مسدود می‌کنند و **رمزنگاری داده‌های حساس** باعث می‌شود حتی در حالت سرقت فایل‌ها، محتوا قابل استفاده نباشد. **کنترل نرم‌افزارهای نصب‌شده** مانع نصب نرم‌افزارهای کرک آلوده[۵] یا ابزارهای ناامن می‌شود.

۴. Data Loss Prevention
۵. Cracked Software
۶. بر اساس گزارش گزارش امنیتی اتحادیه اروپا
Europol 2025 Internet Organised Crime Threat Assessment (IOCTA 2025)
https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf

# ۲ حملات گروه‌های هکتیویستی

رفتار این گروه از مهاجمان نشان می‌دهد که هدف‌شان از حمله و نفوذ، انگیزه مالی نیست؛ به‌نظر می‌رسد که محرک آن‌ها نوعی باور به ایدئولوژی، انگیزه اجتماعی و اعتراضی است. فعالیت‌های رایج این گروه‌ها شامل: حملات DDoS[۷] برای ایجاد اختلال در سرویس‌دهی، تخریب یا Deface صفحات وب، افشای اسناد یا اطلاعات برای ایجاد فشار رسانه‌ای/عملیات روانی یا اطلاعاتی در فضای سایبری/ارسال پیام انبوه از راه سایت‌های پربازدید است.

این دسته از نفوذگران با ایجاد دسترسی روی سامانه‌های پرکاربرد مانند پیام‌رسان‌ها، ارسال پیام انبوه یا سایت‌های خبری و سایت‌های پربازدید، تلاش می‌کنند تا در وقایع اجتماعی یا سیاسی به نفع گروه خاصی حملات خود را پیش ببرند. هم‌چنین در مواردی دیده شده است که این گروه‌ها علاوه‌بر به سرقت بردن اطلاعات، با از بین بردن اطلاعات و ایجاد اختلال گسترده می‌خواهند نوعی ایجاد نارضایتی عمومی یا تخریب برند قربانی را دنبال کنند.

## روش نفوذ رایج

نفوذ به وب‌سایت از راه آسیب‌پذیرهایی مثل تزریق فایل یا ضعف در پلاگین‌ها و Deface ( خراب کردن یا تغییر محتوا دادن) در وب سایت یک کسب‌وکار

## اقدام‌های پیش‌گیرانه

**ایمن‌سازی سامانه‌های وب (Web Hardening) و اجرای تست نفوذ دوره‌ای وب و شبکه**

۷. Distributed Denial of Service حملات انکار سرویس توزیع شده

# ۳ حملات هدفمند پیشرفته

دراین دسته، مهاجمان با هدفی مشخص، مدت‌دار، و برنامه‌ریزی‌شده عمل می‌کنند. بررسی‌ها نشان می‌دهد که آنها دراین نوع حمله‌ها به دنبال اهدافی بیش از کسب مالی و اعتبار هستند، آنها هم‌چنین به‌نظر می‌رسد که منابع و امکانات نامحدود در اختیار دارند. طبق شواهد اغلب این گروه‌ها از سوی سازمان‌های اطلاعاتی، گروه‌های نیابتی و دولت‌ها حمایت و کنترل می‌شوند.

## تهدیدات پیشرفته مداوم (Advanced Persistent Threat APT)

گروه‌های APT مدت‌ها پیش از شروع حمله به بررسی و شناخت کامل تجهیزات، افراد، ساختار سازمان و زنجیره‌ی تامین می‌پردازند و در حملات خود از روش‌های جدید و ناشناخته علیه قربانی استفاده می‌کنند. می‌توان از روش‌های زیر به‌عنوان بخشی از روش‌های رایج این گروه‌ها نام برد: **استفاده از اکسپلویت‌های روز-صفر (Zero-Day)، حملات به زنجیره تامین (تزریق کد مخرب در محصولات جانبی)، فریب اجتماعی بسیار هدفمند و ایجاد زیرساخت کامند و کنترل C2 پایدار.** به عنوان شاخص‌های کلیدی این حملات می‌توان به مواردی مانند **چندمرحله‌ای بودن، فعالیت طولانی‌مدت، استفاده از تکنیک‌های جدید، نفوذ عمیق، باقی‌ماندن در شبکه برای ماه‌ها یا سال‌ها** اشاره کرد. در مواجه با Zero-Day Exploit یا اکسپلویت روز صفر[۸] همه آسیب پذیر هستیم، تنها راه مقابله با آن‌ها، استفاده از تامین کننده‌های مختلف در تجهیزات به‌شکل متوالی است که تنها می‌تواند شانس موفقیت حمله را کاهش دهد. اهمیت این آسیب‌پذیری‌ها تا آن جاست که قیمت خرید و فروش Zero-Day Exploit در دارک وب، در مواردی حتی به چندین میلیون دلار هم می‌رسد.

نکته مهم در حملات فریب اجتماعی بسیار هدفمند که توسط این گروه‌های نفوذگر انجام می‌شود، ایجاد زنجیره‌ای از اطلاعات نادرست درباره زیرساخت‌های فیزیکی ساختگی و شرکت‌های جعلی در شبکه‌های اجتماعی است؛ اقدامی که سطح اعتماد قربانیان را افزایش داده و پیشبرد اهداف نفوذگران را برای بدست آوردن دسترسی اولیه بسیار آسان‌تر می‌کند.

**گروه‌های هکری تنها**
**در حدود یک ساعت پس نفوذ اولیه می‌توانند**
**به حساس‌ترین بخش شبکه**
**شما برسند!**

### روش نفوذ رایج

نفوذ چندمرحله‌ای شامل Spear Phishing، ایجاد درب پشتی یا Backdoor، استفاده از تکنیک‌های حرکت جانبی (Lateral Movement) برای گسترش سطح دسترسی در شبکه.

### اقدام‌های پیش‌گیرانه Threat Hunting مداوم + معماری چندلایه امنیتی (Defense in Depth)

این حملات، پنهان و چندمرحله‌ای‌اند، تنها راه کشف آنها شکار تهدید فعال و پایش رفتارهای غیرعادی مداوم است.

۸. یک نقطه‌ضعف کاملاً ناشناخته در نرم‌افزار یا سیستم که سازنده هنوز از وجودش خبر ندارد و هیچ وصله (Patch) یا راه‌حل امنیتی برای آن منتشر نشده است

# جاسوسی سایبری
## Cyber Espionage

بررسی‌ها نشان می‌دهد که هدف این حملات سرقت اطلاعات حساس دولتی، صنعتی، تحقیقاتی یا سیاسی است و بیشتر روی اهداف خاص مثل سازمان‌ها، وزارتخانه‌ها، پژوهشگاه‌ها، شرکت‌های تکنولوژی تمرکز دارند. این حملات بخشی از عملیات APT هستند. و بیشتر برای به‌دست آوردن طرح‌های تحقیقاتی دارویی و نظامی، اطلاعات محرمانه تجاری، مذاکرات بین‌المللی، پایگاه‌های داده حیاتی یا بسیار فراگیر استفاده می‌شوند.

نکته‌ی مهم دیگر آن است که این حملات معمولا با رفتارهای سازمانی مطابقت پیدا می‌کنند و سرقت اطلاعات به‌مرور زمان و آهسته شکل می‌گیرد و هیچ‌گونه تغییر یا تخریبی در ساختارها به‌وجود نمی‌آید. در مواردی هم که مشکوک به شناسایی شوند، با فرامین از قبل تعبیه شده به‌شکل خودکار ردپا و اثر خود را پاک می‌کنند!

### روش نفوذ رایج

نفوذ چندمرحله‌ای و سرقت تدریجی داده از طریق ارتباطات رمزگذاری‌شده، روش‌های Steganography و تونل‌سازی (VPN معکوس یا Command and Control پنهان بر روی پروتکل‌های رایج UDP, DNS).

### اقدام‌های پیش‌گیرانه  جداسازی شبکه (Segmentation) + کنترل دقیق دسترسی به داده‌های حساس

جاسوسی سایبری بر سرقت تدریجی و آهسته داده‌ها تکیه دارد؛ محدود کردن مسیرهای دسترسی و جداسازی کامل شبکه‌های داخلی از اینترنت، امکان نفوذ و انتقال اطلاعات را بسیار سخت می‌کند.

# خرابکاری سایبری
## Cyber Sabotage

هدف این حملات **ایجاد اختلال یا نابودی زیرساخت‌های کنترلی و صنعتی، در موارد خاص و یا مقیاس بزرگ است.** حمله به زیرساخت‌های حیاتی (برق، آب، حمل‌ونقل، صنعت)، تخریب داده یا تجهیزات زیرساختی، حملات ICS/SCADA، انتشار بدافزارهای ویرانگر (Wiper Malware) از جمله اهداف این گروه‌ها هستند.

در این حملات، تیم‌های نفوذگر با آگاهی کامل از ساختار صنعتی، حملات سایبری را با هدف آسیب زدن به زیرساخت صنایع انجام می‌دهند. اختلال در سامانه‌های تصفیه‌ی آب، اختلال در خط تولید صنایع نظامی و هسته‌ای و همچنین اختلال در شبکه توزیع سوخت، نمونه‌هایی از این حملات است.

### روش نفوذ رایج

مهاجم از شبکه IT وارد می‌شود از طریق یک گذرگاه ارتباطی یا تجهیز میان‌افزار با پیکربندی نادرست به شبکه OT دسترسی پیدا می‌کند و سپس فرمان‌های مخرب ارسال می‌کند.

### اقدام‌های پیش‌گیرانه جداسازی سخت‌گیرانه IT/OT و پایش تخصصی شبکه‌های صنعتی (Industrial IDS/Anomaly Detection)

چون خرابکاری سایبری بر دسترسی عمیق به سیستم‌های صنعتی متکی است، جدا کردن شبکه‌های صنعتی از اینترنت و از شبکه IT و استفاده از ابزارهای تشخیص ناهنجاری صنعتی موثرترین دفاع است. این روش، امکان نفوذ و انتقال اطلاعات را بسیار سخت می‌کند.

# ۴ تهدیدات داخلی

یکی از مهم‌ترین تهدیداتی که ممکن است آن را فراموش کنیم، خطرات ناشی از بی‌احتیاطی درون سازمان است. این تهدیدها را می‌توان در چند گروه، آسیب‌شناسی کرد:

- **کارمندان ناراضی:** افرادی که در بحران‌ها یا پس از اخراج، ممکن است به انتقام‌جویی فکر کنند و در پی خرابکاری باشند.
- **پیمانکاران خارجی:** در مواردی که دسترسی گسترده‌ای به پیمان‌کارها بدون نظارت کافی، داده می‌شود.
- **سهل‌انگاری ناخواسته:** کارمندانی که ناآگاهانه یا به اشتباه، شرایط نفوذ را ایجاد می‌کنند و یا بدون دریافت آموزش‌های لازم طعمه‌ی حملات مهندسی اجتماعی (Phishing Attack) می‌شوند.
- **حساب‌های فراموش‌شده:** دسترسی‌های قدیمی که پس از ترک کارمند قطع نشده باقی می‌ماند.

**بررسی‌ها نشان می‌دهد که این حملات بیشتر در کسب‌وکارهایی رخ می‌دهد که دارایی‌های با نقدشوندگی بالا دارند؛ مانند صرافی‌های آنلاین و پلتفرم‌های رمزارز، و معمولاً انگیزه آن‌ها مالی یا انتقام است.**

## روش نفوذ رایج

دسترسی غیرمجاز کارمند ناراضی، پیمانکاران خارجی به داده‌های حساس یا حذف، تغییر اطلاعات با استفاده از دسترسی قانونی ولی کنترل‌نشده.

## اقدام‌های پیش‌گیرانه

**پیاده‌سازی مدل اعتماد صفر (Zero Trust) + مدیریت چرخه عمر حساب‌ها (IAM/Identity Governance)**

Zero Trust سطح دسترسی کارکنان و پیمانکاران را به حداقل می‌رساند و IAM مانع باقی ماندن حساب‌های قدیمی، دسترسی‌های مازاد و سواستفاده کارمندان ناراضی می‌شود.

۵۲

# برای آمادگی پیش از حمله‌های سایبری چه باید کرد؟

# برای آمادگی پیش از حمله‌های سایبری چه باید کرد؟

در این بخش به مجموعه‌ای از اقدامات پایه‌ای و پیشگیرانه با هدف افزایش سطح مقاومت سازمان در برابر تهدیدات سایبری خواهیم پرداخت. تجربه‌ی تیم‌های «واکنش سریع» نشان می‌دهد که بخش قابل‌توجهی از قربانیان حملات سایبری می‌توانستند فقط با رعایت اصول اولیه و اقدام‌های ساده اما حیاتی، از وقوع خسارات گسترده جلوگیری کنند. هرچند اجرای کامل بسیاری از این راهکارها به زمان، منابع کافی و نیروی متخصص و همچنین تطبیق آن‌ها با شرایط هر کسب‌وکار نیاز دارد.

در این بخش تلاش شده است تا به‌شکل خلاصه و هدفمند مهم‌ترین اقداماتی که هر سازمان فارغ از اندازه و حوزه فعالیت برای حفظ آمادگی و کاهش ریسک باید به آن توجه کند، ارایه شود.

**نکته‌ی مهم**: در ارائه این رویکردها، توجه به وضعیت فعلی کشور و احتمال افزایش حملات سایبری در نظر گرفته شده است. بنابراین تمرکز اصلی این بخش بر اقدامات دفاعی‌ای است که کم‌هزینه، دارای اولویت بالا، قابل اجرا در کوتاه‌مدت و در عین حال مؤثر باشند.

# ۱ سرویس‌های غیرضروری را خاموش کنید

درنظرداشته باشید که هرسرویس یا سیستم اضافه یک سطح حمله است.

بنابراین **از تیم فنی/امنیتی بخواهید:**

- تمامی سرویس‌های آزمایشی، قدیمی و غیرضروری را متوقف و از سیستم حذف کنند.
- قابلیت‌ها و ماژول‌های غیرحیاتی را غیرفعال کنند تا سطح حمله کاهش یابد.
- تمامی APIهای بلااستفاده یا در معرض اینترنت را مسدود یا محدود نمایند.
- سیستم‌های کاری را در زمان استفاده نکردن یا ترک سازمان خاموش کنند.
- پورت‌های پیش‌فرض شناخته‌شده را تغییر داده و دسترسی‌ها را محدود کنند.
- سرویس‌های پیش‌نصب (Default Services) را بررسی و موارد بلااستفاده را غیرفعال کنند.
- به‌شکل دوره‌ای پورت‌ها و سرویس‌های فعال را Audit و بررسی کنند تا چیزی از قلم نیفتد.
- سرویس‌ها و سیستم‌های قدیمی یا بدون پشتیبانی را غیرفعال یا دسترسی به آنها را محدود کنند.

## هدف

کاهش سطح حمله است. هرچه سیستم ساده‌تر باشد، دفاع آسان‌تر است.

# ۲ دسترسی‌ها را محدود کنید

استفاده از اطلاعات حساب‌های افشاشده یکی از رایج‌ترین روش‌ها برای ایجاد دسترسی اولیه و نفوذ به سامانه‌های هدف است.

**از تیم فنی و امنیتی بخواهید:**

- تمامی دسترسی‌های کاربران را بازنگری کرده و بر اساس اصل **حداقل دسترسی** به حداقل ممکن کاهش دهند.
- احراز هویت چندمرحله‌ای (**MFA**) را برای تمامی سیستم‌های حیاتی، VPN، ایمیل، و پنل‌های مدیریتی فعال کنند.
- در وضعیت دورکاری، دسترسی را صرفاً از IP های مشخص و لیست سفید مجاز کنند.
- حساب‌های قدیمی، غیرفعال یا بدون استفاده را حذف و حساب پیمانکاران خارجی را محدود یا زمان‌دار کنند.
- بر روی تمامی تجهیزات حیاتی (Email Systems، Root Access، Active Directory Admins) سیاست اجبار تغییر رمز پس از زمان مشخص فعال شود.
- سیاست رمز عبور پیچیده با حداقل ۱۲ کاراکتر، ترکیب حروف، اعداد و نشانه‌ها اعمال گردد.
- مجوزهای مدیران سیستم و حساب‌های دارای سطح دسترسی بالا را دوره‌ای بازنگری و در صورت عدم نیاز حذف کنند.
- حساب‌های سرویس (Service Accounts/sql server/backup–agent) را بررسی و رمزهای ثابت آن‌ها را به‌شکل دوره‌ای تغییر دهند.
- اعتبارنامه‌ها (Passwords/API Keys) را با ابزارهای (Pwned) در برابر پایگاه‌های افشای عمومی بررسی کنند.

## هدف

هر چه سطح دسترسی‌ها کنترل شده‌تر باشد، شانس موفقیت و گسترش حمله کاهش می‌یابد.

# ۳ از داده‌های حیاتی محافظت کنید

مهاجمان معمولا برای ایجاد بیشترین آسیب اقدام به تخریب داده‌ها، حذف پایگاه‌های اطلاعاتی، از دسترس خارج کردن سیستم‌ها از راه اجرای باج‌افزارها و یا ابزارهای تخریبی می‌کنند. بنابراین حفاظت از داده و پشتیبان‌گیری امن، یکی از مهم‌ترین عوامل بقای سازمان پس از حادثه است.

**از تیم فنی/امنیتی بخواهید:**

- نسخه‌های پشتیبان **آفلاین (Offline/Air-Gapped)** تهیه و نگهداری کنند؛ زیرا مهاجمان به شکل هدفمند نسخه پشتیبان آنلاین را شناسایی و حذف می‌کنند.
- نسخه‌های پشتیبان را در **چند ناحیه جغرافیایی** یا حداقل در دو مرکز داده مجزا نگهداری کنند.
- دسترسی به نسخه‌های پشتیبان را **فقط به‌صورت فیزیکی و آفلاین** محدود کنند و از اتصال آن‌ها به شبکه جلوگیری کنند.
- به‌شکل دوره‌ای **صحت (Integrity) و قابلیت بازیابی (Recoverability)** نسخه‌های پشتیبان را تست و تمرین کنند.
- داده‌ها را طبقه‌بندی و **داده‌های حیاتی و حساس** را با سطوح حفاظت و رمزنگاری قوی‌تر ذخیره کنند.
- از رمزگذاری (Encryption) برای داده‌های در حال ذخیره و انتقال استفاده کنند تا در حالت سرقت، داده‌ها امکان بهره‌برداری نداشته باشند.

## هدف

**بکاپ امن، آخرین و مهم‌ترین شانس بقای سازمان بعد از فاجعه، حمله باج‌افزاری یا تخریب عمدی داده‌هاست.**

# ۴ کارکنان؛ آسیب‌پذیرترین حلقه، موثرترین خط دفاع

کارکنان ناآگاه یا بی‌احتیاط آسان‌ترین نقطه ورود برای مهاجمان هستند

رایج‌ترین تهدیدات علیه کارکنان سازمان شامل موارد زیر می‌شود:

- ارسال ایمیل با لینک جعلی برای سرقت دسترسی
- ارسال ایمیل یا برقراری تماس‌های جعلی از طرف مدیران یا همکاران با هدف ایجاد/تغییر دسترسی
- ارسال لینک‌های آلوده در شبکه‌های اجتماعی، به‌ویژه لینکدین، با عنوان دعوت‌نامه، همکاری، یا پیشنهاد شغلی
- دریافت فایل‌های مخرب از طریق واحدهای پشتیبانی، ارتباط با مشتری یا منابع انسانی

ازکارکنان بخواهید:

- فایل ناشناس، مشکوک یا غیرمنتظره را باز نکنند.
- روی لینک‌های ناشناس یا غیرمنتظره کلیک نکنند.
- هویت فرستنده درخواست‌های حساس را از طریق یک کانال دیگر تایید کنند.
- از محیط کار یا ابزارهای مورد استفاده در شبکه‌های اجتماعی اطلاعاتی منتشر نکنند.
- ابزارهای فیلترشکن، کرک، نرم‌افزارهای نامعتبر، یا نسخه‌های ناشناس را بروی سیستم کاری نصب نکنند.
- رمزها را در فایل‌های شخصی، مرورگر یا ابزارهای نامطمین ذخیره نکنند.
- هر رفتار مشکوک را بدون درنگ و بدون واهمه گزارش دهند؛ به خاطر داشته باشید که اشتباه کردن پذیرفتنی است، گزارش نکردن نه

## هدف

**نیروی انسانی یکی از اصلی‌ترین حلقه‌های زنجیره‌ی تأمین امنیت در سازمان است. با آموزش مناسب می‌توان این نقطه‌ضعف بالقوه را به یک لایه‌ی دفاعی فعال و آگاه تبدیل کرد.**

# ۵ فرض کنید نفوذ انجام شده است

همیشه این فرض را داشته باشید که مهاجم قبلا به سیستم‌های سازمان شما وارد شده است؛ پس، به دنبال محل‌های اختفا یا رفتارهای مشکوک در سامانه‌های حیاتی بگردید. **در حملات APT گروه‌های مهاجم از ۱۰ روز تا ۱ سال قبل از وقوع حمله در شبکه حضور دارند** و رفتارهای سازمانی شما را زیر نظر دارند و در طراحی حمله رفتارهای تیم‌های فنی را در نظر می‌گیرند.

**از تیم فنی/امنیتی بخواهید:**

- ثبت و نگهداری **لاگ‌ها در بالاترین سطح ممکن** در سامانه‌های حیاتی فعال شود.
- لاگ‌های حیاتی به‌ویژه در **لبه‌ی شبکه (Firewalls، Gateways، VPN، IDS/IPS)** در سامانه‌ای جداگانه و خارج از شبکه عملیاتی نگهداری شوند.
- لاگ‌ها به‌شکل **مداوم و فعال** بررسی و تحلیل شوند، نه فقط در زمان وقوع حادثه.
- هرگونه **تغییر غیرعادی در فایل‌های سیستمی، اسکریپت‌ها، سرویس‌ها یا تنظیمات سیستم** به‌عنوان نشانه احتمالی حضور مهاجم بررسی شود.
- دسترسی‌های مشکوک یا غیرمنتظره بدون درنگ، مسدود و بررسی امنیتی انجام شود.
- حساب‌های دارای دسترسی بالا، از جمله **مدیران سیستم، واحد مالی، تیم DevOps و مدیران ارشد** با حساسیت بیشتری پایش شوند.
- رفتارهای غیرعادی، به‌ویژه **در ساعات خارج از زمان کاری، شب‌ها یا تعطیلات** با دقت بررسی شوند.
- **ترافیک رمزگذاری‌شده ناشناخته، ارتباط با مقصدهای غیرمعمول یا الگوهای ترافیکی غیرعادی** شناسایی و تحلیل شود.

## هدف

پایش مداوم سامانه‌ها و تحلیل رفتارها برای شناسایی و پیش‌گیری زودهنگام فعالیت‌های مخرب است. بنابراین بررسی رفتارهای غیرطبیعی را تا رسیدن به علت دقیق رها نکنید.

# ۶ کارمندان ناراضی و پیمانکاران خارجی را جدی بگیرید

در شرایط بحران، کارمندانی که به‌تازگی با آن‌ها قطع همکاری شده است، یا کارکنانی که تحت فشارهای مالی و نارضایتی شغلی قرار دارند، ممکن است به تهدیدات داخلی تبدیل شوند. بررسی‌ها نشان می‌دهد که هرچند نسبت وقوع حملات ناشی از تهدیدات داخلی نسبتاً کم است، اما این نوع حملات از پرهزینه‌ترین موارد محسوب می‌شوند؛ زیرا مهاجم از داخل سازمان یا از طریق دسترسی پیمانکاران وارد شده و معمولاً به منابع حساس‌تری دسترسی دارد.

**از تیم فنی/امنیتی بخواهید:**

- از قطع کامل و فوری همه حساب‌ها، دسترسی‌ها و توکن‌های احراز هویت کارکنان اخراج‌شده یا جداشده از سازمان اطمینان حاصل کنند.
- سیاست‌ها و کنترل‌های امنیتی مرتبط با زنجیره تأمین، پیمانکاران و فروشندگان خدمات را بازنگری و به‌روز کنند.
- دسترسی پیمانکاران، تامین‌کنندگان و نیروهای برون‌سازمانی را فقط براساس کمترین سطح دسترسی لازم و با رویکرد حداقل اعتماد تنظیم کنند.
- دسترسی‌های موقت برای پیمانکاران به‌حالت زمان‌دار ایجاد شود و پس از پایان فعالیت، فورا مسدود گردد.
- دسترسی‌های با ریسک بالا (مانند دسترسی به سامانه‌های مالی، DevOps، دیتابیس‌ها یا کنترل پروژه) تحت پایش مداوم قرار گیرند.
- هرگونه رفتار غیرعادی (مثلا دانلودهای حجیم، دسترسی خارج از ساعت کاری یا تغییرات غیرمنتظره) بدون درنگ بررسی شود.

## هدف

کاهش ریسک نفوذ داخلی و سواستفاده از دسترسی‌ها از راه اعمال کنترل‌های سخت‌گیرانه مبتنی بر **Zero Trust** و مدیریت دقیق چرخه‌ی عمر دسترسی‌های کارکنان و پیمانکاران.

# ۷ آمادگی برای ارایه خدمت در حالت «سرویس محدود»

پس از یک رخداد سایبری، ممکن است امکان ارایه‌ی سرویس کامل وجود نداشته باشد. در چنین وضعیتی، آماده بودن برای ارایه «سرویس محدود» می‌تواند از توقف کامل کسب‌وکار جلوگیری کرده و تجربه کاربران را به شکل کنترل‌شده مدیریت کند.

**از تیم فنی/امنیتی بخواهید:**

- **سطوح مختلف سرویس‌دهی** را به‌شکل شفاف تعریف کنند (سرویس کامل، سرویس محدود، سرویس اضطراری).
- مشخص کنند که **کدام قابلیت‌ها یا ماژول‌ها می‌توانند موقتاً غیرفعال، حذف یا ساده‌سازی شوند** بدون اینکه سرویس به‌طور کامل متوقف شود.
- **تمرین اجرای سرویس محدود** را به‌شکل دوره‌ای انجام دهند تا فرآیند بدون خطا و قابل تکرار باشد.
- **پیام‌ها و سناریوهای از پیش آماده** شده برای اطلاع‌رسانی به کاربران تهیه کنند تا در زمان بحران بتوان سریع، شفاف و حرفه‌ای پاسخ داد.
- مطمین شوند که **زیرساخت لازم برای ارایه سرویس محدود** از پیش طراحی شده است.
- امکان ارایه سرویس با **عملکردهای حیاتی محدود** را بررسی کنند.
- زمان‌بندی و فرآیند بازگشت از سرویس محدود به سرویس کامل را از قبل تعیین کنند.

## هدف

**در وضعیت بحرانی، ارایه سرویس در حالت محدود به مراتب بهتر از خاموشی کامل است.**

# ۸ ارتباط با مشتریان را مدیریت کنید

در دوران بحران، مهم‌ترین دارایی سازمان **اعتماد کاربران** است. انکار، پنهان‌کاری یا کوچک‌نمایی حادثه، نه‌تنها از اثرات یک حمله سایبری نمی‌کاهد بلکه می‌تواند آسیب اعتباری را تشدید کند. آن‌چه می‌تواند اعتبار سازمان را حفظ کند، **پذیرش واقعیت، شفافیت کنترل‌شده و ارتباط مسئولانه با مشتریان** است.

**از تیم فنی و تیم‌های مرتبط بخواهید:**

- سناریوهای مختلف **جبران خسارت مشتریان** (مانند بازپرداخت، تمدید خدمات، یا ارائه خدمات جایگزین) را پیش از وقوع حادثه بررسی و آماده کنند.
- یک **صفحه وضعیت سرویس (Status Page)** مستقل و خارج از زیرساخت اصلی ایجاد کنند تا حتی در زمان اختلال سامانه‌ها نیز قابل دسترس باشد.
- اختلال‌ها و رخدادها را **شفاف، دقیق و به‌موقع** به کاربران اطلاع‌رسانی کنند.
- **کانال‌های ارتباطی جایگزین** (مانند شبکه‌های اجتماعی، ایمیل اضطراری یا مرکز تماس مستقل) برای ارتباط با مشتریان در زمان بحران آماده کنند.
- سیاست‌های **نگهداری داده‌های مشتریان** را بازنگری کنند و **حداقل داده‌های ضروری** را ذخیره کنند تا در صورت رخداد امنیتی، دامنه آسیب کاهش یابد.

## هدف

**در حملات سایبری، بی‌خبری، تأخیر در اطلاع‌رسانی یا انکار واقعیت، اغلب بیش از خود رخداد به اعتبار کسب‌وکار آسیب می‌زند. مدیریت شفاف و مسئولانه ارتباط با مشتریان می‌تواند اعتماد آن‌ها را حتی در شرایط بحران حفظ کند.**

# ۹ از مهم‌ترین سلاح خود استفاده کنید؛ به‌روزرسانی و نصب به‌موقع افزونه‌های امنیتی

اصلی‌ترین سلاح کارشناسان دفاعی در سازمان‌ها به‌روزرسانی و نصب به‌موقع وصله‌های امنیتی است. تاخیر در به‌روزرسانی سیستم عامل‌ها، سامانه‌ها و نرم‌افزارها یکی از رایج‌ترین دلایل موفقیت حملات سایبری است. مهاجمان معمولا از آسیب‌پذیری‌های شناخته‌شده سواستفاده می‌کنند؛ بنابراین هر روز تاخیر، درواقع یک فرصت اضافی برای آن‌ها ایجاد می‌کند!

**از تیم فنی بخواهید:**

- **سازوکار مطمین و پایدار** برای دریافت، آزمایش و توزیع وصله‌های امنیتی ایجاد و عملیاتی کنند؛ این سازوکار باید حتی در شرایط **اختلال یا قطع اینترنت بین‌الملل** نیز قابل اجرا باشد.
- تمام سرویس‌هایی که مستقیما **در معرض اینترنت** هستند را در **اولویت نخست** قرار دهند و وصله‌های این سرویس‌ها را **فوری** اعمال کنند.
- دارایی‌های آسیب‌پذیر یا قدیمی را **ایزوله** و دسترسی‌های آن‌ها را **حداقلی** کنند. اگر مجبور به استفاده از سیستم عامل‌ها یا کتابخانه‌های بدون وصله هستند، باید در محیطی جدا، محدود و کنترل‌شده نگهداری شوند.
- فرآیند مدیریت وصله‌ها (Patch Management) را به‌شکل **نظام‌مند و مستمر** برای تمامی بخش‌ها اجرا کنند، از جمله:
  - سیستم عامل‌های سرور و سیستم عامل‌های کاربران
  - تجهیزات شبکه مانند فایروال‌ها، سوئیچ‌ها و روترها
  - سرویس‌ها و سامانه‌های عمومی و وب‌سرویس‌ها
  - کتابخانه‌ها، بسته‌ها و وابستگی‌های نرم‌افزاری
  - سامانه‌های داخلی و سرویس‌های جانبی که معمولاً کمتر مورد توجه قرار می‌گیرند.

## هدف

**با اعمال سریع وصله‌ها، سطح حمله کاهش می‌یابد و بسیاری از مسیرهای نفوذ بالقوه پیش از آن‌که مهاجمان از آن‌ها سو استفاده کنند بی‌اثر می‌شوند. این کار یکی از کم‌هزینه‌ترین و موثرترین اقدامات برای جلوگیری از نفوذ است.**

# یک آزمون ساده:
# تاب‌آوری سازمان‌مان در برابر حملات سایبری چه اندازه است؟

با توجه به شواهدی که نشان می‌دهد با روند روبه‌افزایش حملات سایبری در کشور و پیامدهای سنگین آن برای کسب‌وکارها، مواجهیم، می‌توان ادعا کرد که ارزیابی منظم میزان تاب‌آوری سازمان‌ها دیگر یک انتخاب نیست، بلکه ضرورتی انکارناپذیر است. چنین ارزیابی‌ای امکان شناسایی ضعف‌های پنهان را پیش از آن‌که به بحران تبدیل شوند، فراهم می‌کند. هرچند استانداردهایی مانند ISO 22301 و ISO/IEC 27001 چارچوب‌های جامع و مؤثری برای این ارزیابی ارایه می‌دهند، اما اجرای کامل آن‌ها معمولا زمان و منابع قابل‌توجهی می‌طلبد. در وضعیت حساس کنونی بر اساس تجربیات میدانی، سازمان‌هایی که هنوز این مسیر را طی نکرده‌اند می‌توانند با پاسخ به چند پرسش کلیدی، ارزیابی سریع و اولیه‌ای از میزان آمادگی و تاب‌آوری خود در برابر حملات سایبری به‌دست آورند.

پرسش‌های مرتبط با این آزمون به شرح زیر است:

۱

## حیاتی‌ترین سرویس‌های کسب‌وکار ما کدام‌اند و چه جایگزینی برای آنها داریم؟

برای پاسخ به این سؤال، **فهرست سرویس‌های حیاتی** را مشخص می‌کند و پایه‌ی طراحی هر برنامه امنیتی، پشتیبان‌گیری و بازیابی بحران است.

### اقدامات پیشنهادی

- فهرست سرویس‌های حیاتی مستند و به‌شکل دوره‌ای بازبینی شود.
- وابستگی‌های هر سرویس مشخص شود.
- برای هر سرویس، راهکار جایگزین در سطوح مختلف آماده شود.
- ظرفیت سرویس‌های جایگزین سنجیده شود.

۲

## اگر پایگاه داده اصلی ما امروز از بین برود، چه اندازه طول می‌کشد تا آن را بازیابی کنیم؟

پاسخ به این سوال، میزان کیفیت نسخه‌های پشتیبان و کارآمدی برنامه‌ی بازیابی پس از بحران را مشخص می‌کند.

### اقدامات پیشنهادی

- RTO (Recovery Time Objective) و RPO برای تمام سامانه‌ها مشخص شود.
- فرآیند بازیابی کامل پایگاه داده به‌شکل دوره‌ای آزمایش شود.
- کیفیت و سازگاری داده‌ها در نسخه‌های پشتیبان بررسی شود.

## ۳

## در وضعیت از بین رفتن داده در سطح مختلف، امکان بازسازی داده‌های حیاتی از منابع دیگر وجود دارد؟

پاسخ به این سوال، تاب‌آوری کسب‌وکار برای بقا در شرایط بسیار سخت را مشخص می‌کند.

### اقدامات پیشنهادی

- داده‌ها بر اساس اهمیت و غیرقابل‌جبران بودن دسته‌بندی و مستندسازی شوند.
- تعیین شود که هر دسته داده از چه منابعی قابل بازسازی است (Logs, Apps, Partners, Devices).
- فرآیند بازسازی عملیاتی مستند شود، نه فقط تئوریک!
- سامانه‌هایی که داده تولید می‌کنند باید دارای یک مسیر ثبت رویداد (Audit Trail) کامل باشند
- برای داده‌های بسیار حیاتی نسخه‌های پشتیبان غیرقابل تغییر (Immutable) طراحی شود.

**تجربه‌ی حملات سایبری کشور در یک سال اخیر نشان داده که در پاسخ به این سوال، همواره بدترین سناریوها را در نظر بگیرید.**

## ۴

## نسخه‌ی پشتیبان و تجهیزات جایگزین در چه سطحی تعبیه شده است؟

در بسیاری از حملات مشاهده شده است که مهاجم علاوه بر تخریب داده‌ها و از بین بردن نسخه‌های پشتیبان، به تجهیزات سخت‌افزاری هم آسیب می‌زند. از طرفی زمانی که سازمان با رخداد سایبری مواجه شود، بسیاری از تجهیزات موجود تا پایان عملیات پاکسازی قابلیت استفاده ندارند و باید تجهیزات جایگزین استفاده کنید.

### اقدامات پیشنهادی

- نسخه‌های پشتیبان در چند ناحیه‌ی مختلف جغرافیایی به‌صورت کاملا مجزا و افلاین نگهداری شوند.
- برنامه‌ریزی برای تامین تجهیزات حیاتی جایگزین (لپ‌تاپ، سرور، فایروال، سوئیچ) انجام شود.
- دیتاسنتر جایگزین از نظر ظرفیت، امنیت و شبکه ارزیابی شود.

## ۵

## اگر دستگاه یکی از کارمندان در واحد (...) هک شود، مهاجم به چه چیزهایی دسترسی پیدا می‌کند؟

پاسخ به این سوال، میزان کنترل دسترسی‌ها را مشخص می‌کند. در بسیاری از سازمان ها، یک حساب کاربری می‌تواند به بخش بزرگی از سیستم، دسترسی پیدا کند.

### اقدامات پیشنهادی

- طراحی و اعمال اصل حداقل دسترسی (Least Privilege) برای تمام نقش‌ها.
- محدودسازی دسترسی‌ها براساس واحد سازمانی، موقعیت، شبکه و ساعت کاری.
- استفاده از احراز هویت چندمرحله‌ای (MFA) برای همه حساب‌ها، مخصوصا ادمین‌ها.
- تفکیک نقش‌های مدیریتی (Admin) از حساب‌های کاربری روزمره.
- بررسی دوره‌ای دسترسی‌های بیش از حد یا غیرضروری.
- استفاده از سامانه تشخیص و واکنش در سطح پایانی (EDR) بروی تمامی دستگاه‌های کارمندان حساس.

## ۶

## چه زمانی می‌توانیم تشخیص دهیم که به ما حمله شده است؟

در بسیاری از حملات، نفوذگران ماه‌ها در سازمان حضور دارند و تیم‌های داخلی تنها پس از وارد شدن خسارت متوجه وقوع حمله می‌شوند. در نبود مانیتورینگ مؤثر و تحلیل مستمر لاگ‌ها، معمولاً حملات پس از اجرا و هنگام بروز اثرات مخرب شناسایی می‌شوند.

### اقدامات پیشنهادی

- جمع‌آوری لاگ‌ها از تمام لایه‌ها: شبکه، سیستم عامل، سرویس‌ها، دیتابیس، Cloud.
- استفاده از راهکارهای مدیریت اطلاعات و رویدادهای امنیتی (SIEM) و ایجاد Use-Case های اختصاصی (به‌جای قوانین عمومی).
- فعال‌سازی هشدار برای رفتارهای مخرب شناخته‌شده و ناشناخته (Anomaly Detection).
- اجرای مانورهای شکار تهدید ادواره‌ای، حتی بدون مشاهده هشدار.
- تعریف شاخص‌های هشدار اولیه (Early Indicators).
- آشنایی تیم داخلی با الگوهای حملات جدید.
- رصد و پایش دائمی تغییرات در سامانه‌ها و حساب‌های حساس.

## ۷
## آیا زیرساخت ما یک نقطه شکست واحد دارد؟

ریسک حمله در آن سرویس و سرور بسیار بالاست. نیاز است که راهکارهای متنوع برای جایگزینی نقاط شکست تدارک دیده شود.

### اقدامات پیشنهادی

- تحلیل کامل Single Points of Failure در شبکه، دیتابیس، DNS، هویت، زیرساخت و اتصال اینترنت.
- طراحی معماری با افزونگی (Redundancy)
- تست دوره‌ای Failover ، نه فقط طراحی آن.
- استفاده از زیرساخت High Availability برای سامانه‌های کلیدی.

## ۸
## اگر امشب یک حمله سایبری رخ دهد، افراد کلیدی چقدر در دسترس هستند و چه کسی فرماندهی و مدیریت حمله را برعهده دارد؟

سرعت و امکان تصمیم گیری در زمان رخداد بسیار مهم است، قبل از بحران باید مسولیت و نقش افراد تعریف شده باشد. همچنین برای تمامی افراد، باید جانشین با اختیارات مشابه تعریف شود تا در وضعیتی که فرد در دسترس نباشد، دیگر افراد بتوانند مسوولیت‌های آن شخص را انجام بدهند.

### اقدامات پیشنهادی

- تعیین فرماندهی رخداد با اختیارات رسمی و مصوب هیات مدیره.
- تعریف جانشین برای تمام نقش‌های کلیدی (Technical, Legal, Communication, HR).
- تعریف مسیرهای ارتباط بحران (Secure Channels).
- ذخیره اطلاعات تماس افراد کلیدی در محلی خارج از شبکه سازمان.

اگر این مسوولیت‌ها قبل از حمله مشخص نباشد، در زمان حمله سایبری، **سازمان از نظر تصمیم گیری فلج می‌شود.**

۰۳

# مدیریت بحران و اقدامات حیاتی در لحظه‌ی بحران سایبری

# مدیریت بحران و اقدامات حیاتی در لحظه‌ی بحران سایبری

از آن‌جا که مواجهه با رخدادهای سایبری برای بسیاری از کسب‌وکارها تجربه‌ای کم‌تکرار است، در لحظه وقوع یک حمله سایبری، سرعت، شفافیت و تصمیم‌گیری درست سه عامل **تعیین‌کننده برای کنترل خسارت و حفظ تداوم کسب‌وکار** هستند. بررسی تجربه حملات اخیر نشان می‌دهد که حتی سازمان‌هایی با بالاترین سطح بلوغ امنیتی نیز ممکن است در یک لحظه دچار اختلال گسترده شوند. تفاوت سازمان‌های تاب‌آور با دیگران، در توانایی آن‌ها برای مدیریت «ساعت صفر» و اجرای مجموعه‌ای از اقدامات هماهنگ، اولویت‌بندی‌شده و قابل اتکا است.

در ادامه مجموعه‌ای از گام‌های ضروری ارایه می‌شود که باید بلافاصله پس از شناسایی حمله اجرا شوند. **هدف این بخش، جلوگیری از گسترش حمله، کاهش حداکثری خسارات، حفظ امنیت داده‌ها و بازگردانی سریع سرویس‌های حیاتی است.** این اقدامات بر اساس تجربه‌های میدانی، استانداردهای مدیریت بحران و تحلیل حملات سایبری تدوین شده‌اند تا مدیران ارشد بتوانند در وضعیت واقعی و تحت فشار، تصمیمات درست و موثر را انتخاب کنند.

# ۱ ساعت صفر: اطلاع از حمله

## وضعیت

متوجه می‌شوید یک حمله سایبری یا رخداد غیرعادی در سامانه‌ها اتفاق افتاده است.

## نکات و اقدامات ضروری

- در این مرحله احتمال انتشار **اطلاعات ناقص، گمانه‌زنی و گزارش‌های غیرقطعی** بسیار بالاست. هر گزاره را با احتیاط و بدون فرض قطعی بودن بپذیرید. **میزان قطعیت** هر خبر را بسنجید: شنیده‌ها، ظن‌ها، شواهد اولیه، یا گزارش فنی مستند؟
- ممکن است برخی اعضای تیم فنی در لحظه در دسترس نباشند. **منتظر آن‌ها نمانید؛** اگر نشانه‌ها با باج‌افزار، پاک‌سازی داده، یا تخریب سرویس‌ها همخوانی دارد، بی‌درنگ وارد فاز **اقدامات مهار فوری** شوید.
- بلافاصله از **رابط امنیت یا فنی** بخواهید در هر ۱۰–۵ دقیقه یک گزارش کوتاه بر مبنای شواهد (نه تحلیل شخصی) ارایه کند.
- تا حد امکان **آرامش خود را حفظ کنید.** واکنش احساسی یا عجله در تصمیم‌گیری می‌تواند باعث از دست رفتن داده یا تشدید بحران شود.
- اجازه بدهید تیم‌ها بدون تنش و دستورهای متناقض کار کنند. در این مرحله **تمرکز و نظم** حیاتی است.
- **منبع شناسایی رخداد** را مشخص کنید (SIEM، EDR، کاربر، مانیتورینگ، هشدار SOC، یا گزارش بیرونی).
- مشخص کنید آیا **شاهد عینی برای نوع حمله** (Log, Alert, Screenshot, Console Message) وجود دارد یا فقط احتمال مطرح شده است؟

## پرسش‌های ضروری که باید از تیم فنی/امنیت پرسیده شود: (پاسخ در این لحظه معمولاً کامل نیست؛ هدف شفاف‌سازی وضعیت اولیه است)

- دقیقاً **چه اتفاقی افتاده** و اولین بار **چه کسی و در چه ساعتی** آن را مشاهده کرده؟
- کدام سرویس‌ها تحت تأثیر قرار گرفته‌اند یا مشکوک به اختلال هستند؟
- **نوع حمله** قابل تشخیص است؟ (باج‌افزار، نفوذ، پاک‌سازی، اختلال سرویس، سوءاستفاده کاربری، خطای فنی، رفتار غیرعادی)
- حمله **از چه زمانی شروع شده** و اکنون در چه مرحله‌ای است؟
- آیا حمله هنوز **فعال** است یا متوقف شده؟ آیا شواهدی از **گسترش به سایر سرورها یا کلاینت‌ها** وجود دارد؟
- آیا داده یا فایل‌هایی **تغییر، حذف، رمزگذاری یا دستکاری** شده‌اند؟ یا آیا نشانه‌ای از **نفوذ به حساب‌های ادمین یا سرویس‌ها** دیده شده است؟

# ۲ اقدام آنی: جلوگیری از گسترش حمله

## هدف

**توقف فوری و کامل پیشروی حمله.** در این مرحله هر ثانیه مهم است؛ از هر روش استاندارد، ایمن و قابل اتکا برای مهار اولیه استفاده کنید.

## وضعیت

شواهد اولیه وقوع یک فعالیت غیرعادی را تایید کرده‌اند، اما ماهیت دقیق حمله و سطح گسترش آن هنوز مشخص نیست.

## نکات و اقدامات ضروری

- در این مرحله **نباید هیچ زمانی را از دست داد.** تأخیر چند دقیقه‌ای می‌تواند به رمزشدن یا نابودی گسترده داده‌ها منجر شود.
- در حملات **باج‌افزار، Wiper، حملات مخرب یا ناشناخته**، اجرای دستورات مهار فوری می‌تواند از قفل شدن یا حذف شدن داده‌های سالم جلوگیری کند.
- سیستم‌ها و سرورهای مشکوک را **بدون هیچ تأخیری ایزوله** کنید: قطع شبکه، جدا کردن کابل، غیرفعال‌سازی کارت شبکه یا جداسازی از سوییچ.
- سرویس‌های حیاتی یا پرخطر را **به‌صورت پیشگیرانه متوقف کنید،** حتی اگر نشانه واضحی از آلودگی ندارند، در صورتی که احتمال انتشار وجود دارد.
- دسترسی‌های از راه دور مانند **SSH، RDP، VPN** و نیز **حساب‌های مدیریتی** را موقتاً مسدود کنید تا از سواستفاده احتمالی جلوگیری شود.
- در شبکه‌های بزرگ، اگر احتمال انتشار سریع وجود دارد، دستور **خاموش کردن فوری تجهیزات اداری و سیستم‌های کارمندان** یک اقدام حیاتی است.
- از هرگونه **پاک‌سازی عجولانه** که ممکن است شواهد جرم‌یابی را از بین ببرد خودداری کنید. اولویت این مرحله **مهار** است، نه پاک‌سازی.
- فرد یا تیمی را تعیین کنید که **زمان، اقدامات انجام‌شده و موارد مشکوک** را دقیقا ثبت کند. این اطلاعات برای تیم‌های فارنزیک و تصمیم‌گیری‌های بعدی بسیار حیاتی است.
- اگر سامانه‌های پایش (SIEM، EDR، Syslog) فعال‌اند، فورا بررسی کنید آیا **الگوهای گسترش حمله در حال افزایش است** یا نه.
- ارتباط تیم‌ها باید کوتاه، دقیق و مستند باشد؛ تصمیم‌های پراکنده یا بدون مسئولیت مشخص می‌تواند بحران را تشدید کند.

# روش‌های مهار فوری

## BlueScreen(BSOD)

### توقف فوری سیستم‌های آلوده

- در سازمان‌هایی که از قبل این روش را تعریف و تمرین کرده‌اند، **موثرترین روش** برای از دسترس خارج کردن یک سرور است.
- نیازمند **دسترسی مستقیم** به سرور یا دیتاسنتر است.
- موجب توقف کامل سیستم‌عامل و فریزشدن محتویات RAM می‌شود؛ این داده‌ها بعدها در اختیار تیم‌های جرم‌یابی دیجیتال قرار می‌گیرد.
- در حملاتی مانند باج‌افزارها، این روش می‌تواند از رمز شدن داده‌های سالم جلوگیری کند.

## قطع برق فیزیکی

### اقدام اضطراری و سریع

- ساده‌ترین و سریع‌ترین گزینه توقف آلودگی سایبری است و از سوی افراد غیرفنی سازمان هم می‌تواند انجام شود.
- احتمال کمی برای آسیب سخت‌افزاری وجود دارد، اما مقایسه هزینه‌ها نشان می‌دهد که **نجات داده‌ها بسیار مهم‌تر از ریسک آسیب تجهیز** است.
- برای سرورهای حیاتی که احتمال آلودگی یا گسترش وجود دارد، این روش یک اقدام کلیدی و مؤثر است.
- تجربه حملات واقعی نشان داده است که در برخی حملات **APT**، میان افزار (Firmware) تجهیزات دستکاری شده و دستورات نرم‌افزاری (یا حتی دکمه پاور) ممکن است کار نکنند؛ در چنین وضعیتی قطع برق تنها راه قطعی است.

## جداسازی فیزیکی شبکه

### قطع اتصال اینترنت و بخش‌های داخلی

- در لحظه بحران، **سرعت** مهم‌ترین عامل است؛ بنابراین قطع فیزیکی کابل یا خاموش‌کردن تجهیزات ارتباطی در برخی سناریوها منطقی‌تر از اقدامات نرم‌افزاری است.
- این اقدام اطمینان می‌دهد که هیچ مسیری برای انتقال آلودگی میان بخش‌های مختلف شبکه باقی نمی‌ماند.
- برای جلوگیری از پخش بدافزار، این روش معمولاً موثرترین اقدام در دقایق اول حمله است.
- حتماً مشخص و ثبت کنید که کدام بخش‌های شبکه، سرویس‌ها یا زیرساخت‌های ارتباطی قطع شده‌اند؛ این اطلاعات به تیم‌های ارزیابی دامنه خسارت کمک می‌کند تا محدوده احتمالی نقطه شروع آلودگی (Patient Zero) و مسیر گسترش حمله را با دقت بیشتری تحلیل کنند.

# ۳ ارزیابی دامنه خسارت

## هدف

تعیین دقیق میزان خسارت، نقاط آلوده، تاثیر حمله بر سرویس‌ها، داده‌ها و جلوگیری از اتخاذ تصمیم‌های عجولانه به‌ویژه خودداری از بازگردانی شتاب‌زده سرویس‌ها پیش از شناسایی کامل دامنه حمله.

## وضعیت

وقوع رخداد سایبری تایید شده و اقدامات مهار اجرا شده است. اکنون باید دامنه خسارت، نقاط آلودگی، شدت حمله و پیامدهای عملیاتی آن به‌شکل دقیق بررسی شود.

## نکات و اقدامات ضروری

- پیش از ورود به این مرحله، **اطمینان کامل حاصل کنید که گسترش حمله متوقف شده است.** اگر هنوز احتمال انتشار وجود دارد، ادامه کار می‌تواند خسارت را شدیدتر کند.
- **تصمیمات مهم را به‌تنهایی یا با عجله نگیرید.** نیروهای کلیدی فنی و مدیران مسئول (و جانشینان آنها) باید در محل یا در جلسه حاضر باشند.
- **جلسه تیم واکنش به حادثه را فوراً تشکیل دهید.** نقش‌ها، مسئولیت‌ها، حوزه تمرکز هر تیم و روش گزارش‌دهی را مرور کنید تا از تصمیم‌گیری‌های موازی یا متناقض جلوگیری شود.
- فضای جلسه را آرام و متمرکز نگه دارید. **تنش، اختلافات قبلی و فشار روانی می‌تواند کیفیت تصمیم‌گیری را کاهش دهد** و بحران را تشدید کند؛ بنابراین مدیریت فضای روانی تیم مهم است.
- **ذی‌نفعان کلیدی، سهام‌داران و هیئت‌مدیره** باید از وقوع حمله مطلع باشند. این کار را با یک پیام کوتاه، دقیق و بدون گمانه‌زنی انجام دهید.
- به‌طور موازی درباره نحوه و زمان **اطلاع‌رسانی به مشتریان، کارکنان و شرکای تجاری** تصمیم‌گیری کنید. این تصمیم باید هماهنگ با تیم فنی و حقوقی باشد تا اطلاعات غلط یا ناقص منتشر نشود.
- **تا زمانی که دامنه خسارت و نوع حمله به‌وضوح مشخص نشده است، هیچ سرویسی را بازگردانی نکنید.** بازگردانی زودهنگام می‌تواند منجر به آلوده‌سازی مجدد یا از دست رفتن داده‌های سالم شود.

## نکات و اقدامات ضروری

- ارزیابی دامنه خسارت ممکن است چندین ساعت یا چند روز طول بکشد. بنابراین **تیمی جداگانه** از تیم ارزیابی تشکیل دهید که:
  - مسوول بررسی نسخه‌های پشتیبان و امکان بازیابی باشد.
  - نسخه‌ی محدود خدمات (Limited Service) را آماده کند.
  - در حالت نیاز طرح ارایه سرویس حداقلی را اجرا کند.
- این کار باعث می‌شود ارزیابی فنی بدون فشار و بر اساس واقعیت‌ها پیش برود.
- برای حداقل **۲۴ ساعت نخست بحران** شرایط مناسب استقرار، تغذیه، استراحت و پشتیبانی را برای نیروهای درگیر فراهم کنید. در حملات سایبری، **کاهش انرژی تیم** یکی از عوامل افزایش خطای انسانی است.
- مدیریت رخدادهای جدی ممکن است از **چند ساعت تا چندین روز** طول بکشد. بنابراین:
  - برنامه‌های سه روز آینده خود را لغو یا به افراد دیگر واگذار کنید.
  - از نیروهای کلیدی بخواهید برنامه‌های روزهای آینده را آزاد کنند.
  - امکان شیفت‌بندی و جایگزینی افراد خسته را پیش‌بینی کنید.
- اگر تیم فنی تجربه کافی در شناسایی ابعاد حمله، تحلیل لاگ‌ها، تفکیک آلودگی و جرم‌یابی دیجیتال ندارد، **از تیم‌های حرفه‌ای / DFIR Incident Response بخش خصوصی** استفاده کنید. در حملات پیچیده، این اقدام ضرر را به شکل چشمگیری کاهش می‌دهد. از طرفی تیم‌های خارجی فشار و استرس نیروهای داخلی را تجربه نکرده‌اند و برای کار در این شرایط آموزش دیده‌اند.
- **تا زمان رسیدن تیم جرم‌یابی دیجیتال از تیم فنی بخواهید که هیچ تغییری اعمال نکند.** راه‌اندازی مجدد، نصب نرم‌افزارها و یا اعمال هر تغییری می‌تواند شواهد تیم‌های جرم‌یابی دیجیتال برای بررسی نوع حمله را از بین ببرد و فرآیند تحلیل را دچار خطا، نقص داده و حتی گمراهی کند.
- از تیم فنی بخواهید **تمامی شواهد، لاگ‌ها، گزارش‌های سیستمی و نشانه‌های آلودگی** را به‌شکل کامل، ساختارمند، در یک محیط امن و بدون تغییر اصل داده‌ها ذخیره کنند. این شواهد برای تحلیل فنی، تصمیم‌گیری اجرایی، اقدامات قانونی و ارایه مدارک معتبر به مراجع ذی‌صلاح حیاتی است.

# ۴ ارتباط با سازمان‌ها و مراجع ناظر بر کسب‌وکار

## هدف

اطلاع‌رسانی سریع و رسمی به مراجع ناظر برای دریافت حمایت تخصصی، کاهش خسارت، هماهنگی در سطح ملی، و ثبت مستندات رسمی رخداد.

## نکات و اقدامات ضروری

- **در اولین فرصت** وضعیت رخداد سایبری را به مرجع ناظر مرتبط اطلاع دهید. نوع مرجع بستگی به حوزه فعالیت شما دارد و می‌تواند شامل موارد زیر باشد:
  - نمایندگان پلیس فتا (کسب‌وکارهای بخش خصوصی)
  - مرکز ماهر (وزارتخانه‌ها، دستگاه‌های دولتی و اجرایی)
  - مرکز راهبردی افتا نهاد ریاست جمهور (نهادهای مالی، زیرساخت‌های حیاتی)
  - سازمان پدافند غیرعامل (زیرساخت‌های انرژی، حمل‌ونقل)
- نمایندگان فنی این مراکز **تجربه و دانش لازم** برای مواجه با رخدادهای سایبری را در اختیار دارند. در بسیاری از حملات، حضور زودهنگام آن‌ها باعث کاهش میزان خسارت شده است.
- هماهنگی با مراجع ناظر کمک می‌کند تا **سایر سازمان‌های مشابه هشدارهای لازم** را دریافت کنند و از وقوع حملات زنجیره‌ای جلوگیری شود؛ به‌خصوص در حملاتی که از یک نوع حمله مشترک (مثل آسیب‌پذیری جدید) سوءاستفاده می‌کنند.
- تهیه صورت‌جلسه رسمی، ثبت زمان‌ها، وضعیت سرویس‌ها، میزان خسارت و اقدامات انجام‌شده همراه با حضور نمایندگان ناظر، در مراحل بعدی، به‌ویژه **پیگیری قضایی، بیمه سایبری، گزارش‌دهی رسمی و پاسخ‌گویی مدیریتی**، بسیار ضروری و موثر خواهد بود.
- ممکن است برخی اعضای تیم فنی نسبت به اشتراک‌گذاری اطلاعات با نمایندگان مراجع ناظر **محتاط یا حساس** باشند. لازم است از آن‌ها بخواهید **نهایت همکاری، شفافیت و هماهنگی** را داشته باشند، زیرا عدم همکاری یا تأخیر در ارائه اطلاعات می‌تواند روند کنترل رخداد را مختل کند.
- بنابراین دقت داشته باشید که اطلاعات ارایه‌شده به مراجع ناظر باید:
  - دقیق، مبتنی بر شواهد و بدون حدس و گمان باشد.
  - در قالب‌های مستند (Log، Report، Snapshot) منتقل شود.
  - با رعایت اصول محرمانگی و طبقه‌بندی داده‌های مشتریان انجام شود.

# ۵ تصمیم‌گیری درباره اطلاع‌رسانی

## هدف

مدیریت بحران با رویکرد شفافیت کنترل‌شده، جلوگیری از ایجاد وحشت و ارایه اطلاعات دقیق، هماهنگ و مبتنی بر شواهد به ذی‌نفعان است.

## نکات و اقدامات ضروری

- **انکار حمله، پنهان‌کاری یا کوچک‌نمایی رخداد** معمولاً آسیب بسیار شدیدتری نسبت به خود حمله ایجاد می‌کند. حتی تأخیر کوتاه در اطلاع‌رسانی می‌تواند اعتماد ذی‌نفعان را از بین ببرد.
- ممکن است سهامداران یا اعضای هیئت‌مدیره به‌دلیل نگرانی از تبعات مالی یا رسانه‌ای، **شما را برای انکار حمله یا انتشار اطلاعات نادرست تحت فشار قرار دهند.** با مشخص کردن پیامدهای حقوقی و اعتباری، اهمیت شفافیت کنترل‌شده را برای آنان روشن کنید.
- اگر در ساعات اولیه رخداد، متوجه شدید **اختلالی ایجاد شده است که مستقیماً بر مشتریان تأثیر می‌گذارد،** از تیم روابط عمومی بخواهید اطلاعیه‌ای کوتاه و دقیق منتشر کند.
- در اولین اطلاعیه به دلیل عدم قطعیت در مورد رخداد، نیازی نیست بر نوع حمله سایبری تاکید کنید، تکذیب هم نکنید کافیست به اختلال اشاره شود:
  - «در این ساعت اختلالی شناسایی شده»، «در حال بررسی فنی هستیم» و «این اختلال کدام سرویس‌ها را تحت تأثیر قرار داده است». پس از جمع‌آوری شواهد و اطلاعات معتبر، **جزئیات دقیق‌تری** درباره ماهیت رخداد ارائه کنید. همچنین به صورت رسمی اعلام کنید که با بررسی‌های فنی و مشخص شدن وضعیت در اطلاعیه‌های بعدی نوع رخداد و وضعیت پایداری سرویس‌ها را اطلاع رسانی خواهید کرد. این رویکرد:
    - از شایعات جلوگیری می‌کند.
    - نشان می‌دهد سازمان رویکرد شفاف و مسئولانه دارد.
    - انتظارات را مدیریت می‌کند.
  - حتماً در اطلاعیه‌ها **راه‌های جایگزین و مطمئن** برای تماس مشتریان‌تان معرفی کنید: کانال اضطراری، شماره پاسخ‌گویی ویژه، سامانه گفت‌وگوی جایگزین، یا صفحه وضعیت مستقل.

## نکات و اقدامات ضروری

- درحالتی که نیاز به ارتباط با رسانه‌ها وجود دارد، **یک سخنگوی رسمی** معرفی کنید تا از انتشار اطلاعات نادرست، چندصدایی یا تناقض جلوگیری شود.
- اگر کسب‌وکار شما با دارایی نقدی مردم (مثل بانک، صرافی، کیف پول، پرداخت الکترونیک) ارتباط مستقیم دارد، آمادگی داشته باشید که **در ساعات اول انتشار اطلاعیه، حجم تماس‌ها، مراجعات تلفنی و حضوری به‌شدت افزایش یابد.**
- باید ظرفیت پاسخ‌گویی، شیفت‌بندی و تیم پشتیبانی را پیش از انتشار اطلاعیه تقویت کنید.
- پس از مشخص شدن ابعاد حمله و دامنه خسارت در اطلاعیه‌های بعدی، یک **زمان‌بندی واقع‌بینانه و مبتنی بر ارزیابی فنی** برای بازگشت سرویس ارایه کنید.
- اگر حمله تاثیری مستقیم بر مشتریان نگذاشته یا نخواهد گذاشت، باید براساس **دامنه خسارت و حساسیت سرویس‌ها** تصمیم بگیرید که اطلاع‌رسانی در چه سطحی لازم است:
  - اطلاع‌رسانی داخلی (کارکنان)
  - اطلاع به مشتریان (در حالت نیاز)
  - اطلاع به واحد حقوقی برای بررسی تعهدات و پیامدهای احتمالی
- در گزارش نهایی، **درس‌آموخته‌ها** و اقداماتی را که برای جلوگیری از تکرار رخداد برنامه‌ریزی شده یا در حال اجراست، شفاف بیان کنید. این اقدامات می‌تواند شامل: بهبودهای فنی، تقویت کنترل‌های امنیتی، اصلاح فرآیندها، آموزش کارکنان و ارتقا یا افزایش ابزارهای مانیتورینگ و تشخیص باشد. این کار نشان می‌دهد سازمان از تجربه رخداد برای افزایش تاب‌آوری خود استفاده کرده است.
- در گزارش نهایی، توضیح دهید چه اقداماتی برای **جبران خسارت یا حمایت از مشتریان آسیب‌دیده** انجام خواهد شد.

# ۶ بازیابی و بازگشت به سرویس

## هدف

مدیریت بازگشت به سرویس قابل اتکا، بازگرداندن کسب‌وکار در سریع‌ترین و پایدارترین حالت ممکن به حالت عادی است.

## وضعیت

دامنه خسارت و ابعاد آن برای تیم فنی احراز شده و اطلاع رسانی اولیه به ذی نفعان صورت گرفته است. نیاز است تا شروع به برنامه ریزی برای بازگشت سرویس های اسیب‌دیده به مشتریان بکنید.

## نکات و اقدامات ضروری

- قبل از هر اقدامی از تیم‌های فنی بخواهید زمان، منابع و پیش‌نیازهای لازم برای بازگرداندن کسب‌وکار به حالت عادی و پایدار را به‌طور دقیق برآورد کنند. این برآورد باید شامل نیروی انسانی، تجهیزات، لایسنس‌ها، پهنای باند، ظرفیت پردازشی و هرگونه ابزار موردنیاز باشد.
- لازم است سناریوهای خوش‌بینانه، محتمل و بدبینانه به‌شکل تفکیک‌شده ارایه شود تا تصمیم‌گیری مدیریتی مبتنی بر واقعیت انجام گیرد.
- بر اساس نوع حمله و سطح خسارت، مشخص کنید که کدام سرویس‌ها با چه اولویتی، در چه بازه‌ی زمانی و با چه سطحی از کیفیت یا محدودیت قرار است عملیاتی شوند.
- در تصمیم‌گیری‌ها، بازگشت مرحله‌ای سرویس‌ها را مدنظر قرار دهید. توصیه می‌شود ابتدا نسخه‌ای محدود و کنترل‌شده از خدمات حیاتی ارایه شود و سپس به‌شکل تدریجی به ظرفیت کامل برسد تا ریسک بروز اختلال مجدد کاهش یابد.
- توجه داشته باشید که ممکن است آسیب‌پذیری یا فایل مخرب در نسخه پشتیبان نیز وجود داشته باشد. بنابراین، قبل از هرگونه بازگردانی، نسخه پشتیبان باید در محیط امن و ایزوله، اسکن و راستی‌آزمایی شود تا از تکرار حادثه جلوگیری شود. هیچ نسخه‌ای بدون تایید رسمی تیم امنیت وارد مدار نشود.
- سرویس‌ها، سرورهاوتجهیزات آلوده را شناسایی کرده و تا زمان بررسی کامل از سوی تیم‌های جرم‌یابی دیجیتال، هرگزوارد مدار نکنید. هرگونه اتصال زودهنگام می‌تواند زنجیره شواهد را مخدوش کرده یا حمله را مجدد فعال کند.

## نکات و اقدامات ضروری

- اطمینان حاصل کنید که پیش از بازگشت سرویس‌ها، آسیب‌پذیری اولیه برطرف شده و مسیر نفوذ کاملاً مسدود شده باشد. بازگردانی بدون حذف ریشه حمله، احتمال تکرار حادثه را به‌شدت افزایش می‌دهد.
- در نظر داشته باشید که در این مرحله، تیم‌های IT و امنیت احتمالاً درخواست افزایش منابع، تجهیزات، نیروی انسانی یا خدمات پشتیبان خواهند داشت. ایجاد محدودیت در این موارد می‌تواند روند بازگشت به سرویس را طولانی کرده و ریسک بروز خطاهای انسانی یا فنی را افزایش دهد. در بحران، تخصیص منابع کافی یک تصمیم راهبردی و نه هزینه اضافی است.
- مطمین شوید که آزمون صحت عملکرد، ارزیابی‌های اضطراری و تست پایداری سیستم‌ها پیش از بازگشت به سرویس انجام شده باشد. این تست‌ها باید شامل سنجش امنیتی، کارکردی، کارایی و یکپارچگی داده‌ها باشد. تایید نهایی باید مستند و قابل ارایه باشد.
- پس از بازگردانی مرحله‌ای سرویس‌ها، برنامه‌ی پایش (Monitoring) ویژه برای ۷۲ ساعت نخست در نظر بگیرید تا هرگونه رفتار مشکوک، خطا یا بازمانده حمله سریعاً شناسایی شود. گزارش این پایش باید به‌شکل منظم به مدیریت ارایه شود.
- با توجه به زمان‌بر شدن مراحل بازگردانی سرویس‌ها، احتمال خستگی و افزایش خطاهای انسانی بالا می‌رود. بنابراین، حتماً به استراحت جسمی و ذهنی تیم فنی توجه کنید و برنامه‌ای برای نوبت‌بندی، استراحت و جلوگیری از فرسودگی آن‌ها در نظر بگیرید. حفظ پایداری تیم فنی، بخشی از مدیریت بحران است.
- در نهایت، تمام اقدامات، تصمیمات و زمان‌بندی‌ها باید به‌صورت کامل مستندسازی شود تا در گزارش‌های رسمی، تعامل با مراجع ذی‌صلاح، بررسی‌های حقوقی احتمالی و همچنین در فرآیند درس‌آموخته‌ها مورد استفاده قرار گیرد.

# ۷ درس‌آموخته‌ها و پیشگیری

## هدف

دستیابی به شناخت دقیق از علت حادثه، رفع ریشه‌ای آسیب‌پذیری‌ها و ایجاد سازوکارهای پایدار برای جلوگیری از تکرار آن.

## وضعیت

سرویس اسیب‌دیده در رخداد سایبری به حالت پایدار درآمده و در حال ارایه خدمت است. نیاز دارید تا اقدامات انجام شده تا این مرحله را مرور کنید و برای جلوگیری از تکرار حادثه برنامه ریزی کنید.

## نکات و اقدامات ضروری

- تحلیل دقیق علت ریشه‌ای حادثه و مسیر نفوذ مهاجم
- مستندسازی کامل یافته‌ها و تجربیات در قالب یک گزارش جامع، قابل‌استناد.
- تدوین و اجرای اقدامات اصلاحی و پیشگیرانه با هدف رفع آسیب‌پذیری‌ها و تقویت فرآیندها و کنترل‌های امنیتی.
- بازنگری و به‌روزرسانی سیاست‌ها، رویه‌ها و دستورالعمل‌های امنیتی براساس نتایج تحلیل حادثه.
- ارتقای سطح آموزش، آگاهی و مهارت کارکنان برای کاهش خطاهای انسانی و افزایش تاب‌آوری سازمان.
- ارزیابی عملکرد تیم پاسخ‌به‌حادثه، شناسایی نقاط بهبود و به‌کارگیری اقداماتی برای ارتقای کارآمدی تیم.
- بهره‌گیری از توان و تجربه تیم‌های متخصص خارج از سازمان در صورت نیاز، به‌منظور تکمیل تحلیل‌ها و افزایش دقت بررسی‌ها.
- تعریف مسوولیت‌ها، زمان‌بندی و منابع موردنیاز جهت اجرای اقدامات پیشگیرانه.
- ارائه و به‌اشتراک‌گذاری گزارش فنی نهایی شامل نتایج، تحلیل‌ها و توصیه‌ها با ذی‌نفعان مرتبط.

# پس از حمله سایبری، گزارش فنی آن را منتشر کنید

انتشار گزارش فنی پس از یک حمله سایبری اهمیت زیادی دارد، چراکه  نسبت به فعالیت سازمان‌تان، شفافیت ایجاد می‌کند و نشان می‌دهد سازمان حادثه را جدی و حرفه‌ای بررسی کرده است. این گزارش کمک می‌کند همه‌ی ذی‌نفعان سازمان مطلع باشند که چه اتفاقی افتاده، علت اصلی حادثه چه بوده، از کجا نفوذ اتفاق افتاده و درنهایت چه خسارتی وارد شده است؟ هم‌چنین، به اشتراک‌گذاری این اطلاعات باعث افزایش آگاهی و جلوگیری از حملات مشابه می‌شود. در نهایت، انتشار چنین گزارشی نشانه مسوولیت‌پذیری و بلوغ امنیتی سازمان است و به حفظ اعتماد مشتریان و شرکا کمک می‌کند.

در پایان یکبار دیگر تکرار می‌کنیم که
امنیت سایبری یک کالا یا خدمت لوکس نیست؛ یک زیرساخت حیاتی است.

به ازای هر کاربر، هر خط کد، هر کارمند و هر بیت داده، باید برای حفظ و ارتقای آن سرمایه‌گذاری کنید.

انجمن
تجارت
الکترونیک
تهران

TEHRAN