



Borna Network Managers  
مدیران شبکه برنا

# خبرنامه برنا



## اخبار حوزه امنیت و شبکه (دی ۱۴۰۴)

در ماه اخیر، قطعی و محدودیت‌های گسترده اینترنت در کشور، چالش‌های تازه‌ای را پیش روی سازمان‌ها و تیم‌های فناوری اطلاعات قرار داده است. بسیاری از راهکارهای امنیتی که سال‌ها بر پایه اتصال پایدار به اینترنت، سرویس‌های ابری و پشتیبانی برون‌سازمانی طراحی شده بودند، در عمل با کاهش اثربخشی یا حتی از کارافتادگی مواجه شده‌اند.

در چنین شرایطی، مفهومی که بیش از هر زمان دیگری اهمیت پیدا می‌کند، تاب‌آوری امنیت سایبری و اتکا به راهکارهای مستقل و بومی است؛ راهکارهایی که بدون وابستگی به اینترنت نیز بتوانند از داده‌ها، دسترسی‌ها و زیرساخت‌های حیاتی سازمان محافظت کنند.

ویژه مدیران و کارشناسان شبکه و امنیت

### چشم‌انداز تهدیدات سایبری در شرایط فعلی

برخلاف تصور عمومی، قطع اینترنت الزاماً به معنای کاهش تهدیدات سایبری نیست. در بسیاری از سازمان ها، تمرکز تهدید از حملات بیرونی به سمت تهدیدات داخلی (Insider Threats) تغییر کرده است. نبود نظارت لحظه‌ای، کاهش Visibility و اختلال در ابزارهای مانیتورینگ، می‌تواند زمینه‌ساز موارد زیر شود:

- نشت داده‌های حساس توسط کاربران داخلی
- سوءاستفاده از دسترسی‌های سطح بالا
- انتقال غیرمجاز اطلاعات از طریق رسانه‌های فیزیکی
- عدم امکان بررسی دقیق رخدادها پس از وقوع Incident

در یک معماری امنیتی استاندارد و چندلایه (Defense in Depth)، ابزارهایی نظیر فایروال، آنتی‌ویروس، EDR و XDR به‌عنوان خط اول دفاعی وظیفه جلوگیری از نفوذ و شناسایی تهدیدات را بر عهده دارند. این لایه‌ها با تمرکز بر شناسایی بدافزار، رفتارهای مخرب و حملات شبکه‌ای، نقش حیاتی در کاهش سطح حمله ایفا می‌کنند.

با این حال، تجربه رخدادهای امنیتی نشان می‌دهد که هیچ‌یک از این ابزارها مصونیت صددرصدی ایجاد نمی‌کنند. عبور مهاجم از لایه‌های اولیه، بروز خطای انسانی یا شکل‌گیری تهدید از درون سازمان، سناریوهایی کاملاً محتمل هستند.

در چنین شرایطی، راهکارهای PAM به‌عنوان لایه کنترل دسترسی‌های حساس و مهار حرکت جانبی مهاجم عمل می‌کنند و در نهایت، DLP به‌عنوان آخرین خط دفاع از داده‌های حساس وارد عمل می‌شود.

DLP تمرکز خود را نه بر شناسایی مهاجم، بلکه بر محافظت از داده در لحظه خروج قرار می‌دهد؛ جایی که حتی پس از وقوع نفوذ نیز می‌توان از نشت اطلاعات جلوگیری کرد.





## Data Loss Prevention (DLP)

### Privileged Access Management (PAM)

به مدیریت و نظارت بر حساب‌های دارای دسترسی سطح بالا می‌پردازد؛ حساب‌هایی که در صورت سوءاستفاده، بیشترین آسیب را به سازمان وارد می‌کنند.

### چرا PAM در شرایط بحران اهمیت دوچندان دارد؟

در شرایطی که:

- MFAهای خارجی در دسترس نیستند.
- دسترسی‌های اضطراری افزایش پیدا می‌کند.
- نظارت سنتی بر فعالیت ادمین‌ها دشوار می‌شود.

نبود PAM می‌تواند منجر به:

- استفاده دائمی از دسترسی‌های Privileged
- نبود لاگ معتبر از فعالیت‌ها
- عدم امکان پاسخ‌گویی پس از رخداد امنیتی

مجموعه‌ای از سیاست‌ها و ابزارهاست که با هدف شناسایی، پایش و جلوگیری از نشت اطلاعات حساس طراحی شده است. این اطلاعات می‌تواند شامل داده های مالی، اطلاعات مشتریان، اسناد محرمانه سازمانی یا داده‌های حیاتی عملیاتی باشد.

### چرا استفاده از DLP در شرایط قطعی اینترنت حیاتی‌تر است؟

در نبود اینترنت، بسیاری از مسیرهای کنترل‌شده خروج داده غیرفعال می‌شوند، اما در عوض مسیرهای آفلاین و داخلی به تهدید اصلی تبدیل می‌شوند:

- انتقال اطلاعات از طریق USB و هارد اکسترنال
- پرینت اسناد حساس
- اشتراک فایل در شبکه داخلی
- کپی و انتقال داده بین سیستم‌ها
- ...و...

راهکارهای DLP کارآمد باید بتوانند بدون وابستگی به سرویس‌های ابری، این رفتارها را شناسایی و کنترل کنند.

### چالش راهکارهای DLP

بسیاری از محصولات DLP:

- نیازمند به‌روزرسانی آنلاین مداوم هستند.
- وابستگی جدی به Cloud دارند.
- در محیط‌های ایزوله یا Air-Gap کارایی مطلوبی ندارند.

### قابلیت‌های کلیدی PAM مؤثر

یک راهکار PAM مناسب باید شامل موارد زیر باشد:

- Password Vault امن
- Session Recording و ثبت کامل فعالیت‌ها
- Just-In-Time Access
- فرآیند تأیید دسترسی (Approval Workflow)
- گزارش‌دهی دقیق و قابل استناد

راهکارهای پیشرفته PAM همچون ARCON امکانات فوق را مازاد بر بسیاری از قابلیت‌های مختلف موجود در راهکار به صورت On-Prem در اختیار شبکه قرار خواهند داد.

### جمع‌بندی

شرایط فعلی کشور نشان داد که امنیت سایبری وابسته به اینترنت، امنیت پایداری نیست. سازمان‌هایی که به دنبال حفظ دارایی‌های اطلاعاتی خود هستند، باید به سمت معماری‌های دفاعی چندلایه و مستقل حرکت کنند.

در این مسیر، راهکارهای DLP, XDR, NDR, EDR و PAM نه ابزارهای لوکس، بلکه ضرورت‌های حیاتی محسوب می‌شوند؛ به ویژه زمانی که این راهکارها بر پایه توان داخلی طراحی شده باشند و بتوانند در سخت‌ترین شرایط نیز به فعالیت خود ادامه دهند.



## خبرنامه امنیت سایبری - دی ماه

اما انسان؛ همچنان ضعیف‌ترین حلقه زنجیره امنیت است.

در نهایت، هیچ راهکار فنی بدون آموزش و آگاهی کارکنان کامل نخواهد بود. آمارهای جهانی نشان می‌دهد بخش عمده‌ای از حملات موفق، ریشه در خطای انسانی دارد؛ از کلیک روی لینک‌های فیشینگ گرفته تا استفاده از رمزهای عبور ضعیف یا اشتراک‌گذاری ناآگاهانه اطلاعات.

برنامه‌های آموزش و افزایش آگاهی امنیت سایبری، به ویژه در کشورهای در حال توسعه، نقشی اساسی در کاهش این ریسک ایفا می‌کنند و باید همزمان با پیاده‌سازی ابزارهای فنی مورد توجه قرار گیرند.

### جمع‌بندی:

چالش امنیت سایبری در کشورهای در حال توسعه، نتیجه عقب‌ماندن امنیت از سرعت تحول دیجیتال است. تا زمانی که امنیت به‌عنوان بخشی جدایی‌ناپذیر از توسعه فناوری در نظر گرفته نشود، این شکاف عمیق‌تر خواهد شد. ترکیب معماری‌های مدرن امنیتی، ابزارهای متناسب، کنترل دسترسی، و آموزش نیروی انسانی می‌تواند این مسیر پرریسک را به مسیری پایدارتر و امن‌تر تبدیل کند.

شرکت مدیران شبکه برنا با بیش از ۱۰ سال سابقه تخصصی در حوزه امنیت اطلاعات و زیرساخت شبکه، به عنوان یکی از مجموعه‌های فعال و قابل‌اعتماد در این حوزه، خدمات خود را متناسب با نیاز سازمان‌ها، شرکت‌ها و کسب‌وکارهای در حال رشد ارائه می‌دهد.





### سخن پایانی

در پایان؛ امیدواریم این رزومه بتواند نمایی شفاف از توانمندی‌ها؛ حوزه‌های تخصصی و خدمات ما ارائه دهد و زمینه ساز همکاری‌های حرفه‌ای و مؤثر با سازمان شما باشد. آماده ایم تا در کنار شما؛ گامی مطمئن در مسیر توسعه و امنیت برداریم.

شرکت «مدیران شبکه برنا» با پشتوانه‌ای از تجربه و دانش تخصصی و تمرکز بر ارائه راهکارهای نوین امنیت شبکه همواره تلاش کرده است تا نیازهای امنیتی سازمان‌ها و شرکت‌ها را در بالاترین سطح پوشش دهد. ما با بهره‌گیری از محصولات و فناوری‌های برتر جهانی در حوزه‌های 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 داده‌های سازمان‌ها را تضمین می‌کنند بلکه امکان مدیریت هوشمند تهدیدات؛ انطباق‌پذیری با الزامات قانونی و افزایش بهره‌وری فناوری اطلاعات را نیز به همراه دارند. در این مسیر؛ تیم فنی متخصص؛ پشتیبانی سریع و ارائه مشاوره دقیق؛ ارزش‌های محوری شرکت ما به شمار می‌آیند. ما باور داریم که امنیت سایبری صرفاً یک محصول نیست؛ بلکه یک تعهد دائمی و یک رویکرد حرفه‌ای برای حفظ سرمایه‌های اطلاعاتی سازمان‌هاست. شرکت مدیران شبکه برنا همواره همراهی قابل اعتماد برای سازمان‌ها و مدیران فناوری اطلاعات بوده و خواهد بود.