وضعیت زرد – هشدار حملات بی‌سابقه سایبری به شبکه‌های کشور از طریق ریموت دسکتاپ (آمادگی برای مقابله)

در روزهای پایان سال ۹۷ ، شبکه‌های شرکت‌ها و سازمان‌های سراسر کشور، با حجم بسیار زیاد و بی‌سابقه‌ای از حملات باج‌افزاری و تحرکات هک و نفوذ مواجه شدند. بیشتر این حملات از طریق سرویس ریموت ودر برخی موارد حتیVPN ها و ابزارهای ریموت انجام گرفته‌اند.

از این جهت پادویش با اعلام هشدار جدی وضعیت زرد امنیتی، توجه عموم کاربران بخصوص مدیران محترم شبکه‌ها و مسئولین فاوا را به نکات ایمنی و امنیتی زیر معطوف می‌دارد) .پشتیبانی شبکه ، فیبرنوری ، کابل کشی(

با جدیت در پیگیری و توجه به رعایت مسائل امنیتی، انتظار می رود آمادگی بیشتری برای مقابله با این حملات در شبکه‌ها به وجود آمده و از این حملات در امان بمانند.

در ادامه نکات مهم برای یادآوری بیان شده است:

۱ .تهیه پشتیبان به‌روز از اطلاعات حیاتی

وجود یک پشتیبان به روز، که به صورت آفلاین نگهداری شودراه اول در بازگرداندن سیستم‌ها به وضعیت عادی بعد از حمله است. بنابراین توصیه می‌شود که یکبار دیگر کل سیستم‌های حیاتی خود را مرور کنید و از اطلاعات آن‌ها پشتیبان گیری کرده و پشتیبان‌ها را به صورت آفلاین نگهداری نمایید. دقت داشته باشید که با گرفتن نسخه پشتیبان، امکان بازیابی پشتیبان‌ها را تست نمایید تا بعداً دچار مشکل نشوید) .مجازی سازی(
علاوه بر سیستم‌های اطلاعاتی و عملیاتی، گرفتن پشتیبان از تجهیزات شبکه شامل روترها، سوییچ‌ها، فایروال، و سایر سیستم‌های مهم مانند اکتیودایرکتوری نیز فراموش نشود.

۲ .غیرفعال کردن فوری راه‌های ارتباطی از طریق ریموت که باعث کاهش درجه خطر تا حد ممکن می شود.

تقریبا در تمامی حملات اخیر هکرها از سرویس ریموت دسکتاپ (Remote Desktop) ویندوز برای نفوذ اولیه خود به سیستم استفاده کرده‌اند. همچنین نفوذ از طریق VPN یا ابزارهای ریموت کلاینتی (مانند AnyDesk و ابزارهای مشابه) نیز متداول است. بنابراین بهتر است به طور موقتی این راه‌ها را غیرفعال کنید یا حداقل آن‌ها را با پسوردها و پالیسی‌های سختگیرانه‌تر (مانند محدودیت آی‌پی) محدود کنید.
همچنین مراقب ابزارهای ریموت کلاینتی مانند AnyDesk و نمونه‌های مشابه را که ممکن است روی یک سرور یا کلاینت باز مانده باشند ، باشید(Voip).

۳ .بررسی سیاست‌های شبکه و محدودسازی تا حد امکان

در وضعیت زرد نیاز هست که یکبار دیگر سیاست‌های امنیت شبکه را مرور نمایید و از اینکه این سیاست‌ها از اصل حداقل دسترسی پیروی می‌کنند اطمینان حاصل کنید. پورت‌های باز اضافی و غیرضروری را ببندید. تا حد امکان سرویس‌های غیرضروری را نیز غیرفعال نمایید.
در مقابله با باج‌افزار، فراموش نکنید که فولدرهای اشتراکی را ببندید یا دسترسی کاربران را به حالت فقط خواندنی محدود نمایید.

۴ .فعال کردن سیستم‌های لاگبرداری و Auditing

اگر خدای نکرده حمله‌ای رخ دهد، برای بررسی منشاء حمله (جهت کشف نقاط نفوذ و جلوگیری از وقوع مجدد) و میزان تخریب و پیشروی حمله (جهت بازگرداندن سرویس‌ها و حذف درب‌های پشتی) به انواع لاگ‌های Audit نیاز خواهید داشت.

بنابراین از فعال بودن لاگ‌های Audit در تجهیزات شبکه و نیز سیستم‌عامل‌های خود اطمینان حاصل کنید. در ویندوز نیاز هست لاگ‌های Security و System فعال باشند. توصیه ما این است که لاگ Audit Process Creation را نیز روی Group Policy فعال نمایید. همچنین میزانی از فضای هارد دیسک را برای ذخیره این لاگ‌ها در نظر بگیرید.

۵ .به‌روز کردن سیستم‌عامل و نرم‌افزارها

کمترین کاری که برای امن کردن سیستم انجام می‌شود بروزرسانی سیستم‌عامل، بروزرسانی نرم‌افزارهای سرویس‌دهنده (وب، ایمیل، اشتراک فایل ...) و نرم‌افزارهای امنیتی مانند ضدویروس و ... است. در وضعیت زرد لازم است دقت و وسواس بیشتری در این مورد داشته باشید تا از آسیب‌پذیری‌های شناخته‌شده عمومی در امان بمانید و سطح آسیب‌پذیری را کاهش دهید.

۶ .اطمینان از عملکرد سیستم‌های امنیتی، مانیتورینگ و هشداردهی آنها

آخرین توصیه: لاگ‌های سیستم‌های خود را مرور کنید و گوش به زنگ رویدادهای نامتعارف (ریموت‌های خارج ساعت کاری یا از کشورهای خارجی و ...) باشید).مانیتورینگ (

طبعا لازم است مجددا از عملکرد سنسورهای امنیتی مانند IDS, WAF و ضدویروس‌ها و نیز نرم‌افزارهای مانیتورینگ اطمینان حاصل کنید تا به محض رخداد اتفاق امنیتی از آن مطلع شوید. بد نیست سیستم هشدار این نرم‌افزارها را نیز تست کنید تا از عملکرد صحیح آن‌ها مطمئن شوید).نصب آنتی ویروس(

در پایان، لازم به تأکید است که این هشدار وضعیت زرد در پاسخ به حملات گسترده و رویدادهای واقعی اخیر اعلام شده که در کمین همه شبکه‌های کشور است. آمادگی برای این نوع حملات قطعاً در پیشگیری یا کاهش ریسک آنها موثر خواهد بود) .دکل مهاری(