روش هایی برای ارتقای امنیت شبکه های کامپیوتری

در لایه شبکه[1]

۱- همیشه از سوییچ قابل مدیریت[2] در شبکه داخلی استفاده کنید. مهمترین مزیت این سوییچ ها امکان بخش بندی[3] شبکه می باشد. برای مثال بهتر است ترافیک دیتای واحد مالی شرکت از واحد مهندسی جدا باشد و یا اینکه ترافیک وب سرویس ها از ترافیک شبکه داخلی جدا گردد[4]. برای این منظور از قابلیت VLAN در سوییچ ها استفاده می شود.

۲- ترافیک وایرلس از شبکه کابلی جدا باشد و نیز ترافیک وایرلس کاربران مهمان از وایرلس کارمندان جدا باشد. برای این منظور می توان از روش های متعددی نظیر Virtual SSID ، ACL و . . . استفاده نمود.

۳- سرویس ها و پورت های غیر ضروری و بدون استفاده در شبکه غیر فعال و بسته شوند. برای مثال جهت جلوگیری از حملات بر پایه Net Bios بهتر است پورت های ۱۳۹ و ۴۴۵ بر روی لبه خارجی[5] شبکه، که می تواند یک روتر یا یک مودم روترباشد، بسته شوند.

۴- از دیگر قابلیت های کاربردی و مفید سوییچ های قابل مدیریت می توان به ایجاد محدودیت بر روی پورت های شبکه اشاره کرد. برای مثال پورت شماره ۴ سوییچ تنها با MAC Address سیستم آقای فلانی کار کند و یا پورت های خالی غیر قابل استفاده باشند.

۵- استفاده از یک UTM[6] مناسب همیشه نقش به سزایی در امنیت شبکه داخلی دارد. پیکربندی قابلیت IDS/IPS بر روی این دیوایس ها فراموش نشود.

۶- در مورد پیاده سازی روش هایی چون partially collapse DMZ یا Honey Pot تحقیق کنید.

---

[1] Network Layer
[2] Manageable switch
[3] Segmentation
[4] DMZ
[5] Edge
[6] Unified Threat Management

در لایه برنامه[7]

۱. سرویس های غیر ضروری و بدون استفاده بر روی سیستم عامل متوقف[8] باشند.

۲. آنتی ویروس نقش به سزایی در جلوگیری از آلوده شدن سیستم به انواع بد افزارها دارد. البته چگونگی پیکربندی آنتی ویروس بسیار حایز اهمیت می باشد. برای مثال بهتر است دسترسی های سیستمی به برخی فایل ها بر روی آنتی ویروس ها بسته شود. (رجوع شود به مقاله "روش های مقابله با باج افزارها" در وب سایت شرکت ارتباطات پرشیا)

۳. توصیه می شود از نسخه های آنتی ویروس با قابلیت فایروال[9] بر روی کلاینت ها استفاده شود.

۴. به روز رسانی سیستم عامل، برنامه های کاربردی و آنتی ویروس همیشه می بایست در اسرع وقت انجام شود.

۵. از مکانیزم های احراز هویت[10] مناسب در شبکه استفاده شود. بسته به نوع و امکانات شبکه می توان از یک یا چند روش احراز هویت استفاده کرد.

۶. پسورد کاربران به ویژه کاربر مدیر شبکه دوره ای عوض شود.

۷. استفاده از سرویس ها و پروتکل هایی نظیر HTTPS ، SSL ، VPN ، IPsec ، NPS ، Radius ، IAS و . . . همیشه توصیه می گردد.

۸. سیستم گزارش گیری بر روی کلاینت ها و سرورهای شبکه پیکربندی گردد.

۹. تا جای ممکن از نصب برنامه های بدون لایسنس یا مجانی در شبکه خودداری کنید.

۱۰. استفاده از روش های پشتیبان گیری متنوع بر روی کلاینت ها، سرورها و پلت فرم مجازی توصیه می گردد.

---

[7] Application Layer
[8] Stop
[9] Business edition
[10] Authentication Authorization Accounting (AAA)

در لایه فیزیکی[11]:

۱) مدیریت بر روی پورت های ورودی سیستم ها در یک شبکه همیشه امری ضروریست. یک کاربر ناراضی و یا ناشی می تواند خطری بالقوه برای شبکه باشد. مانیتورینگ پورت های USB یا CD-ROM و یا در صورت نیاز، بستن آن ها لازم می باشد.

۲) رک حاوی سرور و سوییچ ها همیشه باید قفل بوده و جز مدیر شبکه کسی به آن دسترسی فیزیکی نداشته باشد.

۳) بهتر است دسترسی به اتاق سرور برای همگان امکان پذیر نباشد.

۴) سه راهی برق[12] داخل رک بوده و از بیرون بدان دسترسی نباشد.

۵) مودم شبکه در مکانی غیر قابل دسترس برای همگان قرار داشته باشد.

آموزش کاربران:

- یکی از روش های متداول هکرها به خصوص باج افزارها برای نفوذ به سیستم های شبکه از طریق ارسال ایمیل برای کاربران می باشد. ایمیل های ناشناس و پیوست های این ایمیل ها نباید توسط کاربران باز شوند.
- در خصوص عواقب دادن پسورد به همکاران دیگر، اطلاع رسانی شود.
- کاربران نسبت به پیغام های آنتی ویروس که به صورت Pop-up باز می شود، حساس باشند.
- ورود به سایت های متفرقه و نامعتبر قدغن باشد.
- نحوه استفاده مناسب از سیستم به کاربران، ضمن آموزش مستندسازی شده و در دسترس ایشان قرار بگیرد.

[11] Physical
[12] PDU