تسلط بر مفاهیم پایه شبکه منطبق با استانداردهای بین‌المللی

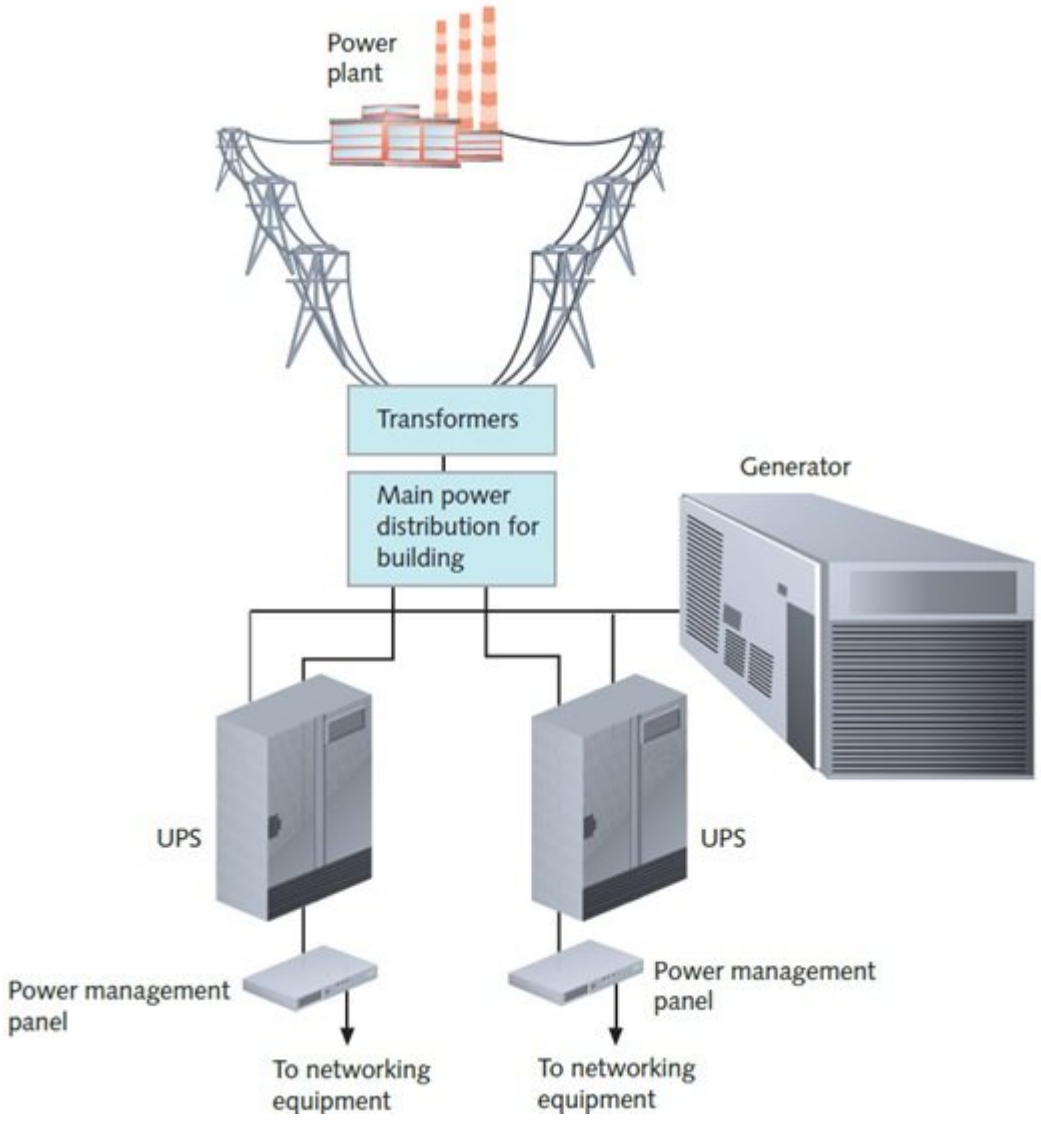
آموزش رایگان دوره نتورک‌پلاس (Network+) (بخش 64)

در شماره گذشته آموزش نتورک‌پلاس با ذخیره‌ساز تحت شبکه، انواع مختلف RAID، شبکه محلی ذخیره‌سازی و فناوری‌های مختلف ارائه شده برای آن، مدیریت انرژی، رخنه‌های مستتر در تامین انرژی و یو پی اس آشنا شدیم. در این شماره مبحث فوق را ادامه خواهیم داد.

برای مطالعه بخش شصت و سه آموزش رایگان و جامع نتورک پلاس (Network+) اینجا کلیک کنید

ژنراتورها

ژنراتور به عنوان یک منبع تامین انرژی قدرتمند به کار می‌رود که در صورت قطعی کامل برق، انرژی لازم برای روشن نگه داشتن دستگاه‌ها را تامین می‌کند. سوخت مورد نیاز ژنراتورها را سوخت‌های دیزلی، گاز پروپان مایع، گاز طبیعی و.... تامین می‌کنند. ژنراتورهای استاندارد می‌توانند با کمترین نوسان انرژی مورد نیاز را تامین کرده و به عنوان یک منبع تامین کننده انرژی ایمن و پایدار در ISPها یا مراکز داده شرکت‌های ارائه دهنده خدمات مخابراتی به کار گرفته شوند. در واقع، در این محیط‌ها، ژنراتورها با UPSهای بزرگ ترکیب می‌شوند تا اطمینان حاصل شود انرژی موردنیاز همیشه در دسترس قرار دارد. در صورت قطعی برق، UPS برق را تا زمانی که ژنراتور شروع به کار کند و به ظرفیت کامل خود برسد، که به‌طور معمول بیش از سه دقیقه نمی‌شود، تأمین می‌کند. اگر سازمان شما به یک ژنراتور برای نیروی پشتیبان متکی است، اطمینان حاصل کنید که باک آن پر بوده و سوخت با کیفیتی درون آن قرار دارد. شکل زیر، زیرساخت تامین انرژی یک شبکه را نشان می‌دهد (شبیه به یک مرکز داده) که از ژنراتور و UPSهای دوگانه استفاده می‌کند. از آنجایی که یک ژنراتور انرژی DC تولید می‌کند، باید یک مولفه برای تبدیل برق تولید شده به AC وجود داشته باشد تا بتوان انرژی تامین شده را به زیرساخت موجود AC انتقال داد تا انرژی موردنیاز یک مرکز داده تامین شود. قبل از انتخاب یک ژنراتور ابتدا نیازهای سازمان خود را برای انتخاب درست ژنراتور محاسبه کنید. همچنین برآورد کنید که چه مدت زمانی ممکن است ژنراتور مجبور شود انرژی ساختمان را تامین کند. بسته به میزان کشش، یک ژنراتور با ظرفیت بالا می‌تواند تا چند روز انرژی موردنیاز را تامین کند. ژنراتورهای گازی یا دیزلی می‌توانند بین 10،000 هزار تا 3،000،000 میلیون دلار (برای کاربردهای صنعتی بزرگ) قیمت داشته باشند.



پاسخ‌گویی و بازیابی

علیرغم انجام هرگونه اقدام احتیاطی، همواره احتمال بروز بلایای طبیعی و نقض‌های امنیتی وجود دارد. آموزش و آمادگی می‌تواند توانایی شما در پاسخگویی و سازگاری با این شرایط را بهبود بخشد. برای آن‌که در آمادگی کامل قرار داشته باشید و بتوانید نیازهای شبکه‌ای کاربران را پیش‌بینی کنید باید در مورد شرایط و موقعیت‌های خاص همچون موارد زیر اطلاع داشته باشید.

• حادثه - هر رویداد، بزرگ یا کوچکی که اثرات نامطلوبی روی نحوه دسترسی به شبکه یا منابع آن بگذارد را یک حادثه می‌گوییم. حادثه می‌تواند یک نقص امنیتی مانند دسترسی هکر به یک حساب کاربری، یک آلودگی، مانند یک کرم یا ویروس یا یک مشکل طبیعی همچون آتش‌سوزی یا سیل باشد.

• فاجعه - نوع شدیدتر حادثه است که قطع شدن دسترسی به شبکه را شامل می‌شود که روی فعالیت بیش از یک سیستم یا گروهی از کاربران تاثیر منفی می‌گذارد.

برای مقابله با هر یک از این پیشامدهای ناگوار باید امکانات لازم همراه با تیمی که تجربه مدیریت این شرایط را دارند در دسترس قرار داشته باشد تا مشکلات به سرعت برطرف شده و اشتباهات به حداقل برسد. برای این منظور ابتدا باید با خط‌مشی‌های پاسخ‌گویی و سپس تکنیک‌هایی که برای بازیابی و برطرف کردن فاجعه استفاده می‌شوند آشنا شوید.

خط‌مشی‌های واکنشی نسبت به حوادث به‌طور خاص مجموعه‌ای از ویژگی‌های مرتبط با یک رویداد را مشخص می‌کند

که این ویژگی‌ها است که یک حادثه را به عنوان یک پدیده مخرب تعریف می‌کند. حوادث احتمالی مواردی همچون ایجاد وقفه، آتش‌سوزی، مشکلات اورژانسی مرتبط با اوضاع جوی، حمله هکری، کشف محتوای غیر قانونی روی کامپیوتر یک کارمند یا انجام کار غیرقانونی از سوی یک کارمند، شیوع بدافزار یا بلاهای طبیعی که فعالیت کسب‌وکار را در مقیاس گسترده و به‌طور کامل متوقف می‌کند را شامل می‌شود. خط‌مشی‌ها با هدف حفظ امنیت مردم نوشته می‌شوند. محافظت از اطلاعات حساس؛ اطمینان از در دسترس‌پذیری و یکپارچگی شبکه و جمع‌آوری داده‌ها به منظور تحلیل عاملی که باعث بروز حادثه شده است، فردی که مسئولیت بروز حادثه متوجه او است و اقداماتی که باید در آینده برای جلوگیری از حادثه‌های مشابه لحاظ شوند، در این خط‌مشی تعریف می‌شوند. پاسخ‌گویی به یک حادثه فرآیندی شش مرحله‌ای است که به شرح زیر انجام می‌شود.

مرحله 1، آماده شدن: تیم پاسخ‌گویی به وقایع احتمالی باید برنامه‌ریزی‌های اولیه را انجام داده باشد. این فرآیند نصب سیستم‌های پشتیبان و جمع‌آوری تمامی اطلاعات مورد نیاز برای بازگرداندن شبکه به حالت اولیه که مواردی همچون گذرواژه‌ها، پیکربندی، فهرست فروشندگان، مکان ذخیره‌سازی نسخه پشتیبان از داده‌ها، اطلاعات تماس اضطراری، قوانین مربوط به حفظ حریم خصوصی و SLAها را شامل می‌شود.

مرحله 2 تشخیص و شناسایی: از آنجایی که سامانه‌های هشداردهنده امنیتی و محیطی می‌توانند همه موارد را تشخیص دهند، کارکنانی که مستقیما با برنامه‌ریزی مرتبط با پاسخ‌گویی به حوادث مرتبط نیستند باید در ارتباط با مشکلات بالقوه و کارهایی که پس از بروز مشکلات باید انجام دهند آموزش‌های لازم را فراگیرند.

مرحله 3، محدوده: تیم برای محدود کردن آسیب‌ها باید برنامه‌ریزی‌هایی را انجام داده باشد. سامانه‌های آلوده یا آسیب دیده باید جدا شوند و کارکنان تیم پاسخ‌گویی فراخوانده شوند تا مشکل به سرعت برطرف شود.

مرحله 4: شناسایی علت بروز مشکل: تیم باید عاملی که باعث بروز مشکل شده است را شناسایی کرده و برای مشکل پیدا شده راه‌حلی را ارائه کند تا آلودگی یا آسیب به سایر بخش‌های شبکه سرایت نکند.

مرحله 5: بازیابی: به مجموعه عملیاتی اشاره دارد که شرایط را به حالت عادی باز می‌گرداند. این فرآیند تعمیر سامانه‌های آسیب دیده و بازگرداندن آن‌ها به حالت قابل استفاده را شامل می‌شود.

مرحله 6، بازبینی: تیم تعیین می‌کند که چه نکات ارزشمندی از حادثه باید مستندسازی شوند تا از اطلاعات فوق برای پیشگیری از بروز مشکلات آتی استفاده کرد.

دقت کنید در بحث خط‌مشی‌های پاسخ‌گویی شما باید به چهار موضوع اعزام کننده (شخصی که برای اولین بار هشداری را ارسال کرده است)، متخصص پشتیانی فنی (فردی در تیم که تمرکزش تنها روی حل مشکل در سریع‌ترین زمان ممکن است)، مدیر (فردی که مسئولیت رسیدگی به امور و تخصیص درست منابع برای حل مشکل بر عهده او است) و متخصص روابط عمومی (در صورت لزوم فردی که باید به عنوان سخن‌گو حاضر شده و برای مردم شرایط را تشریح کند) رسیدگی شود.

برنامه‌ریزی برای بازیابی پس از فاجعه

بازیابی پس از فاجعه به فرآیند بازگرداندن قابلیت‌های حیاتی و داده‌های حساس به شبکه پس از قطع دسترسی که بیش از یک سیستم یا گروهی از کاربران را تحت تاثیر قرار داده است اشاره دارد. یک برنامه‌ریزی مرتبط با بازیابی پس از فاجعه برای سناریوهایی که جنبه بحرانی دارند همچون اقدامات خرابکارانه جدی انجام می‌شود. طرح‌های احتمالی باید برای بازگرداندن یا جایگزینی سیستم‌های کامپیوتری و برق، خط‌مشی‌های مشخصی را تعریف کنند. هدف از برنامه بازیابی پس از فاجعه، اطمینان از تداوم کسب‌وکار است که توانایی شرکت در ادامه فعالیت‌های تجاری با کمترین میزان وقفه ممکن را تضمین کند. یک سازمان می‌تواند از راهکارهای مختلفی برای بازیابی پس از فاجعه استفاده کند. گزینه‌های پیش روی سازمان‌ها بر مبنای میزان مشارکت کارکنان، سخت‌افزارها، نرم‌افزارها، برنامه‌ریزی‌ها و سرمایه‌گذاری قرار دارند. برنامه بازیابی پس از خرابی شبکه‌ها به سه گروه hot site، warm site و cold site تقسیم‌بندی می‌شوند.

Cold site: به کامپیوترها، دستگاه‌ها و اتصالات مورد نیاز برای بازسازی شبکه اشاره دارد که به درستی پیکربندی، به‌روزرسانی یا متصل نشده‌اند و از این‌رو فرآیند بازیابی روی آن‌ها زمان‌بر خواهد بود.

Warm site: به کامپیوترها، دستگاه‌ها و اتصالات لازم برای بازسازی مجدد شبکه موجود اشاره دارد که برخی از مولفه‌ها پیکربندی، به‌روزرسانی یا متصل هستند.

Hot site: به کامپیوترها، دستگاه‌ها و اتصالات مورد نیاز برای بازسازی مجدد شبکه موجود اشاره دارد که همه آن‌ها به‌طور مناسب پیکربندی، به‌روزرسانی و متصل شده‌اند و همگی با وضعیت فعلی شبکه سازگاری دارند. برای یک چنین شبکه‌هایی فرآیند بازیابی پس از فاجعه در کوتاه‌ترین زمان ممکن انجام می‌شود. برای سازمان‌هایی که نمی‌توانند خرابی و قطعی دسترسی به شبکه را تحمل کنند، رویکرد فوق بهترین گزینه برای بازیابی پس از فاجعه است که البته به دلیل این‌که به یک نظارت دقیق و مستمر نیاز دارند، معمولا هزینه‌بر هستند.

حفظ و جمع‌آوری اطلاعات و شواهد

در مدت زمان بروز برخی از حوادث، لازم است یکسری داده‌ها جمع‌آوری شوند تا در صورت لزوم به مراجع قضایی تحویل داده شوند تا اگر فعالیت خرابکارانه‌ای رخ داده یا فردی به عمد عملکرد شبکه را با اختلال روبرو کرده است، پیگیری قانونی امکان‌پذیر باشد. برخی از داده‌های قانونی به دلیل عدم مدیریت صحیح ممکن است آسیب دیده یا نابوده شده باشند که همین مسئله فرآیند تجزیه و تحلیل اطلاعات را با مشکل روبرو می‌کند. در حالت ایده‌آل، یک سازمان باید از وجود یک چند فرد پاسخ‌گو که آموزش‌های لازم را اخذ کرده یا مدارک قابل قبولی دارند که نشان می‌دهد این افراد در زمینه جمع‌آوری و رسیدگی به شواهد به دست آمده متحبر هستند و ادله آن‌ها برای ارائه در دادگاه قابل قبول است جذب شوند. با این حال، بسیار مهم است که هر تکنسین فناوری اطلاعات در یک شرکت از این موضوع اطلاع داشته باشد که چگونه اطلاعات حساس، داده‌های ثبت شده و سایر مدارک قانونی را باید حفظ کند تا زمانی که تیم واکنش سریع به حواث به مدارک نیاز دارند، مدارک لازم را در اختیارشان قرار دهد. اگر به یاد داشته باشید در بخش‌های اولیه آموزش **نتورک‌پلاس** به شما گفتیم که مستندسازی چگونه باید انجام شود، اطلاعات چگونه باید طبقه‌بندی شوند، گزارش‌نویسی چیست و چرا مستندسازی فرآیند مهمی است. تیم پاسخ‌گویی به حوادث بر مبنای مجموعه‌ای از شواهدی که در ادامه به آن‌ها اشاره خواهیم کرد، سعی می‌کند علت بروز حادثه را کشف کند:

1.Secure the area: برای جلوگیری از خراب شدن مدارک و شواهد، هر دستگاه مرتبط با شبکه باید ایزوله شده باشد. این حرف به این معنا است که ارتباط دستگاه با شبکه باید جدا شود (کابل اترنت قطع یا آنتن وای‌فای غیرفعال شود) و اطمینان حاصل شود که هیچ فردی با سیستم در تماس نخواهد بود تا وقتی که تیم پاسخگویی به محل وارد شوند. در حالت ایده‌آل، بهتر است سیستم بدون آن‌که برنامه‌ها بسته شده یا فایل‌های باز بسته شوند به حال خود رها شود. سیستم‌عامل‌های مختلف روش‌های مختلفی برای خاموش کردن دستگاه در اختیار دارند، به‌طوری که داده‌های قانونی حفظ شوند، بنابراین فرآیند خاموش کردن باید به کارشناسان تیم پاسخ‌گویی به حوادث سپرده شود. با این حال، اگر یک برنامه مخرب در حال اجرا است که ممکن است مدارک را از بین ببرد، سریع‌ترین و امن‌ترین راه‌حل این است که سیم برق را از پشت دستگاه (نه فقط از دیوار) جدا کنید.

2. Document the scene: تهیه و تدوین یک پرونده ممیزی شده و قابل دفاع از عملکرد سازمان یکی از مهم‌ترین کارهایی است که برای ارائه به مراجع قانونی باید آماده کنید. مستندسازی کارهایی که همواره انجام می‌شوند باید در هر زمانی انجام شود. به‌طور مثال، اگر دستگاه را به دلیل اینکه یک ویروس هارددیسک را پاک کرده، از دستگاه جدا شده، زمان آن باید مشخص شود و نشانه‌های مشاهده شده به صورت مکتوب توصیف شده باشند که نشان دهند چرا شما هارددیسک را از دستگاه جدا کرده‌اید. همچنین، باید فهرستی از افرادی که به سامانه دسترسی دارند تهیه شوند.

3. Monitor evidence and data collection- نظارت بر شواهد و داده‌هایی که جمع‌آوری شده‌اند حائز اهمیت است. مراقب باشید تمام شواهد موجود در حالت اولیه خود قرار داشته باشند. سعی نکنید برای جمع‌آوری مدارکی که در قالب فایل روی یک کامپیوتر یا سرور قرار دارند به سامانه ورود پیدا کنید، زیرا تغییرات فراداده‌ای در فایل‌ها را به وجود می‌آورد و می‌تواند در دادگاه غیر قابل قبول تلقی شود.

4. Protect the chain of custody- تمام داده‌های جمع‌آوری شده باید به دقت پردازش و ردیابی شوند تا در هر مرحله از ثبت در پرونده وجاهت قانونی خود را از دست ندهند.

5. Monitor transport of data and equipment- به‌طور کلی، تیم واکنش سریع به حوادث مسئولیت انتقال همه مدارک به مراجع قضایی را عهده‌دار است. هرگونه مدرکی باید با دقت مستندسازی و بررسی شوند تا مدارک به

شفاف‌ترین شکل قابل ارائه باشند. برای این منظور بد نیست مدارک در یک آزمایشگاه تخصصی بررسی شوند.

6. Create a report- آماده باشید در مورد تمام فعالیت‌هایی که در مدت زمان پاسخ‌گویی به حادثه انجام داده‌اید گزارشی تهیه کنید. بهتر است، یادداشت‌ها را به شکل گام به گام تهیه کرده باشید و گزارش خود را در اسرع وقت پس از حادثه، در حالی که هنوز جزییات در ذهن شما تازه هستند مکتوب کنید. همه این اطلاعات به احتمال زیاد در گزارش نهایی قانونی لحاظ خواهند شد، بنابراین مهم است گزارش فوق دقیق و کامل آماده شود.

توجه داشته باشید که خط‌مشی‌ها به تنهایی نمی‌توانند از شبکه‌ها در برابر مهاجمان محافظت کنند. مدیران شبکه باید به طراحی فیزیکی، طراحی شبکه، آسیب‌پذیری‌های NOS که در شماره‌های گذشته به آن‌ها اشاره کردیم دقت نظر ویژه‌ای داشته باشند. ما در همین‌جا مبحث بازیابی و بررسی عملکرد شبکه‌ها را به پایان می‌رسانیم و همچون گذشته متذکر می‌شویم که لازم است درباره هریک از مباحثی که به آن‌ها اشاره شد تحقیق جامعی داشته باشید تا بدون مشکل بتوانید آزمون **نتورک‌پلاس** را پشت سر بگذارید.

در شماره آینده آموزش **نتورک‌پلاس** به سراغ مبحث شبکه‌های گسترده خواهیم رفت.

تاریخ انتشار:

30 خرداد 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/15595/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-%D8%B1%D8%A7%DB%8C%DA%AF%D8%A7%D9%86-%D8%AF%D9%88%D8%B1%D9%87-%D9%86%D8%AA%D9%88%D8%B1%DA%A9%E2%80%8C%D9%BE%D9%84%D8%A7%D8%B3-network-%D8%A8%D8%AE%D8%B4-64