National Cyber Security Centre
a part of GCHQ

امنیت سایبری
پاسخ و بازیابی

چگونه برای یک حادثه سایبری آماده شویم، از پاسخ تا بهبودی

فهرست

معرفی

طبیعی است که همه سازمان‌ها با دست اندازها درجاده مواجه شوند. به عنوان مثال یک کسب و کار در بریتانیا تقریباً 50درصداحتمال دارد که شما با یک نقض سایبری مواجه شوید. هنگامی که اتفاق غیرمنتظره ای رخ می دهد، مانند یک حادثه سایبری، دانستن اینکه چگونه باید واکنش نشان داد دشواراست. به طور طبیعی، شما می خواهید مشکل را دراسرع وقت حل کنید تا بتوانید تجارت را به حالت عادی از سر بگیرید

به این دلایل، NCSC این راهنمای کسب و کارکوچک را ایجاد کرده است پاسخ و بازیابی. این به سازمان‌های کوچک تا متوسط راهنمایی می‌کند که چگونه واکنش خود را آماده کنند و برای بازیابی خود دریک حادثه سایبری برنامه‌ریزی کنند. این یک قطعه همراه برای راهنمایی ما درمورد نحوه محافظت از خود در برابر حملات سایبری است

اگرکسب‌وکاربزرگ‌تری هستید یا با تأثیر بیشتری ازیک حادثه سایبری مواجه هستید، بخش مدیریت حادثه در10 مرحله برای امنیت سایبری2 می‌تواند به واکنش سایبری شما کمک بیشتری کند. اعضای هیئت مدیره باید به راهنمای ما در مورد برنامه ریزی واکنش شما به حوادث سایبری مراجعه کنند

حادثه چیست؟

NCSCیک حادثه سایبری را به عنوان دسترسی غیرمجاز(یا تلاش برای دسترسی) به سیستم های ITسازمان تعریف می کند. اینها ممکن است نقض (زمانی که از دسترسی غیرمجازبه داده ها یا سیستم ها آگاه هستید) یا حملات مخرب (مانند حملات انکارسرویس، عفونت بدافزار، باج‌افزاریا حملات فیشینگ)، یا می‌توانند به سادگی رویدادهای تصادفی باشند (مانند آسیب ناشی ازآتش‌سوزی/سیل/ سرقت).

گزارش حوادث

اگر یک حادثه زنده را تجربه می کنید، بلافاصله با Action Fraud تماس بگیرید

0300 123 2040 و 9 را روی صفحه کلید خود فشار دهید. با این کارتماس شما در اولویت قرارمی گیرد و رویداد زنده شما از طریق تلفن تریاژمی شود. بعداً حادثه شما به اداره ملی اطلاعات کلاهبرداری NFIBمنتقل می شود که گزارش شما را بررسی می کند و طیف وسیعی از تحقیقات را انجام می دهد، سپس ممکن است به آژانس پلیس مربوطه منتقل شود. شما ازوضعیت گزارش خود مطلع خواهید شد. اگرسازمان شما قربانی یک حمله سایبری قابل توجه بوده است4، NCSC توصیه می کند که با گزارش این حادثه به ما شروع کنید.

گام 1:

آمـــــاده شـــــدن بـــــرای حـــــوادث

رویدادهای پیش‌بینی نشده، چه بدخواه و چه تصادفی، می‌توانند به طرق مختلف رخ دهند. بنابراین توسعه دستورالعمل‌های گام به گام دقیق برای مدیریت هر نوع حادثه غیرعملی است، زیرا فهرست می تواند بی‌پایان باشد. درعوض، باید کسب و کار خود را برای متداول ترین تهدیداتی که با آن مواجه هستید، با برنامه ریزی برای رسیدگی به آن حوادثی که احتمال وقوع آنها وجود دارد، آماده کنید.

سیستم‌ها و دارایی‌های حیاتی را شناسایی کنید اطلاعات الکترونیکی مانند جزئیات تماس، ایمیل‌ها، تقویم‌ها و اسناد ضروری را شناسایی کنید. دریابید که این اطلاعات در کجا ذخیره می شود. آیا روی دستگاه تکی در دفتر شما وجود دارد؟ آیا روی سرور راه دور است؟ آیا توسط شخص ثالث در ابر ذخیره می شود؟

نقطه عمل: یک نسخه پشتیبان روزانه/هفتگی منظم از آن تهیه کنید اطلاعات ضروری. به طور مرتب تست کنید که نسخه پشتیبان کار می کند برای اطمینان از اینکه می توانید اطلاعات را از آن بازیابی کنید

در مرحله بعد، شناسایی کنید که چه فرآیندها و سیستم‌های تجاری برای ادامه فعالیت سازمان شما حیاتی هستند. به عنوان مثال، وب سایتی که مشتریان شما در آن سفارش می دهند، یا تجهیزات تولیدی که توسط رایانه استفاده می کنید. اگر قبلاً این کار را انجام نداده‌اید، این سیستم‌ها و فرآیندهای کلیدی را در اسرع وقت شناسایی کنید و محل ذخیره آنها (یا نحوه دسترسی به آنها) را ثبت کنید.

نقطه اقدام: مسئولیت مشترک را به شخص دیگری هم اختصاص دهید تا اطمینان حاصل کنید که وقتی در دسترس نیستید (مثلاً در تعطیلات یا دور از کار) پوششی وجود دارد. اطمینان حاصل کنید که اسناد کلیدی در دسترس هستند و به روز هستند تا در صورت غیبت شما بتوان آنها را با سایر افراد مرتبط به اشتراک گذاشت/یاد گرفت.

در نهایت، از قبل به این فکر کنید که چگونه می توانید شهرت را به حداقل برسانید

خسارت در صورت وقوع حادثه با کدام شرکای کلیدی باید صحبت کنید؟ ایجاد یک رابطه خوب با شرکای خود، جایی که شما به طور منظم قبل از وقوع یک رویداد صحبت می کنید، در صورت وقوع یک حادثه، کار را بسیار راحت تر می کند.

نقطه اقدام: فهرستی از شرکای کلیدی (مشتریان، تامین کنندگان، اشخاص ثالث، و غیره) تهیه کنید که در نتیجه انواع مختلف حوادث باید با آنها تماس بگیرید. به عنوان مثال، شما باید تماس بگیرید اگر داده‌های پرداخت به خطر افتاد، مشتریان و بانک‌ها، درصورت حمله به حساب‌های شرکتی، تامین‌کنندگان، و اگر اطلاعات شخصی مشتری به سرقت رفت باشد.

خطر را اولویت بندی کنید و آن را مدیریت کنید.

در نظر بگیرید که اگر شما چه اتفاقی می افتاد دیگر به سیستم‌ها یا دارایی‌های مهمی که شناسایی کرده‌اید دسترسی نداشتید. برای درک بهتر مطلب بالا:

- آنچه برای کسب و کار شما مهم است
- چرا مهم است، و
- کاری که شما برای محافظت از آنها انجام می دهید

- می توانید در جایی که به بیشترین محافظت نیاز دارید اولویت بندی کنید. اگر برای شناسایی «جواهرات تاج» خود (یعنی چیزهایی که برای سازمانتان ارزشمند هستند) به کمک بیشتری نیاز دارید، لطفاً به راهنمای ما در مورد تعیین خط پایه خود و شناسایی آنچه که بیشتر به آن اهمیت می‌دهید مراجعه کنید.

ریسک را در دستور کار قرار دهید

بحث در مورد ریسک سازمانی (آنچه برای شما ارزشمند است و چه کاری برای محافظت از آن انجام می دهید) باید بخشی از تجارت عادی باشد. زمانی را برای بحث در مورد این موارد در جلسات مدیریت یا جلسات هفتگی خود اختصاص دهید. درمقایسه با تهدیدات فیزیکی (مانند سرقت و سرقت سهام)، سیل، اقدامات قانونی، سلامت و ایمنی، متوجه شوید که تهدیدات امنیت سایبری در لیست اولویت قرار دارند. گام‌هایی که برای کاهش ریسک کسب‌وکار خود انتخاب می‌کنید باید متناسب با ریسک‌هایی باشد که انجام می‌دهید، و البته مقرون به صرفه.

سازمان هایی که در حال بررسی بیمه سایبری هستند باید بدانند که این بیمه از شما در برابر حمله محافظت نمی کند، اما ممکن است منابع اضافی را در حین و پس از یک حادثه در اختیار شما قرار دهد. بنابراین بیمه سایبری می تواند به عنوان یک ابزار مدیریت ریسک اضافی در نظر گرفته شود، اما برای موارد زیر زمان می برد:

- دامنه و مقیاس پوشش ارائه شده را درک کنید
- اطمینان حاصل کنید که قادر به برآوردن الزامات عملیاتی هستید که توسط بیمه گذار برای شما تعیین شده است

یک طرح حادثه تهیه کنید

اطمینان حاصل کنید که اطلاعات مهمی را که در بالا شناسایی کرده‌اید در مکانی امن نگهداری می‌کنید تا در صورت سرقت یا آسیب دیدن تجهیزات شما توسط یک حمله سایبری، بتوانید از آن‌ها استفاده کنید. مطمئن شوید که می‌دانید در صورت از دست دادن اطلاعات، مانند حمله باج‌افزار، چگونه یک نسخه پشتیبان را بازیابی کنید و به افراد مربوطه در سازمان خود آموزش دهید تا بتوانند همین کار را انجام دهند. وظایفی را به اعضای کارکنان اختصاص دهید، و مستند کنید که در صورت وقوع یک حادثه، هرکدام از مسئولیت‌ها به عهده چه کسی است و چگونه می‌توان با آنها تماس گرفت.

نقطه اقدام: بهترین راه برای آزمایش درک کارکنان از آنچه در طول یک حادثه مورد نیاز است، از طریق تمرین است. برای آزمایش خود از محصول رایگان Exercise in a Box NCSC استفاده کنید تا آماده‌گی سازمان‌ها را بسنجید.

"نقاط محرک" احتمالی حادثه، مانند زمانی که مالکیت یک اقدام یا تصمیم بین افراد منتقل می شود را درک و مستند کنید. به عنوان مثال، یک کارمند ممکن است این اقدام را برای شناسایی مشکلی در وب سایت داشته باشد، اما پس از انجام این کار، چه کسی تصمیم می گیرد که آیا وب سایت باید بسته شود؟ برنامه شما باید مشخص کند که در چه مرحله ای مدیریت ارشد باید درگیر شود.

فهرستی از افراد خارجی ایجاد کنید که باید با آنها تماس بگیرید و می توانند به شما در شناسایی یک حادثه کمک کنند. به عنوان مثال، ارائه دهنده میزبانی وب، خدمات پشتیبانی فناوری اطلاعات یا ارائه دهنده خدمات ابری. جزئیات قرارداد را مستند کنید، از جمله مواردی که پوشش داده شده است، چگونه آنها می توانند به شما کمک کنند، و در چه مرحله ای باید با آنها درگیر شوید. آماده بودن و داشتن اسناد مربوطه در دسترس و به روز می تواند در زمان شما پس از حادثه صرفه جویی کند.

نقطه اقدام: آیا به روزترین اطلاعات تماس را برای کسانی که باید با آنها تماس بگیرید دارید؟ آیا در مکان مناسب ذخیره شده و دسترسی به آن آسان است، در نظر داشته باشید که وسایل ارتباطی عادی شما ممکن است در طول یک حادثه مختل شود؟

به موقع برنامه ریزی کنید تا این جزئیات را هر چند ماه یکبار یا در صورت لزوم بررسی کنید.

اگر بیمه سایبری دارید، جزئیات بیمه‌گر خود را از جمله شماره بیمه‌نامه و هرگونه اطلاعات خاصی که ارائه‌دهنده شما درخواست می‌کند، مستند کنید. هر گونه انطباق قانونی یا نظارتی را که باید به آن پایبند باشید، درک کنید و هر دستورالعمل/خط مشی/قوانینی را که برای شما تعیین می کند را اجرا کنید. باید بررسی کنید که آیا انجمن صنفی شما خطوط راهنمایی یا مشاوره ای دارد که می توانید برای کمک به شما در این شرایط با آنها تماس بگیرید.

گام 2:

آنچه درحال وقوع است را شناسایی کنید

اولین گام در برخورد موثر با یک حادثه شامل شناسایی آن است. یعنی چگونه می توانید تشخیص دهید که حادثه ای رخ داده است (یا هنوز درحال وقوع است)؟

ببینید آیا مورد حمله قرارگرفته اید

مواردی که ممکن است نشان دهنده یک حادثه سایبری باشد عبارتند از:

- کامپیوترها به کندی کار می کنند
- دسترسی کاربران به حساب های خود قفل شده است
- عدم دسترسی کاربران به اسناد
- پیام هایی که برای انتشار فایل های شما باج می خواهند
- افرادی که شما را از ایمیل های عجیب و غریبی که از دامنه شما خارج می شوند مطلع می کنند
- جستجوهای اینترنتی هدایت شده
- درخواست برای پرداخت های غیرمجاز
- فعالیت غیرعادی حساب

دریابید چه اتفاقی افتاده است

10 سوال زیر می تواند به شما کمک کند تا بفهمید چه اتفاقی افتاده است. این نقطه شروعی است که به محض مشکوک شدن به اشتباه از آن می توانید برای جمع آوری اطلاعات حیاتی استفاده کنید. پاسخ ها به شما کمک می‌کند اطلاعات ضروری را به تیم فناوری اطلاعات داخلی یا خارجی خود که مشکل را حل می‌کنند ارائه دهید و بخشی از حادثه شما را تشکیل می‌دهد.
گزارش درس آموخته ها

10 سوال مهم

1. چه مشکلی و توسط چه کسی گزارش شده است؟
2. چه سرویس‌ها، برنامه‌ها و/یا سخت‌افزاری کار نمی‌کنند؟
3. آیا نشانه هایی وجود دارد که داده ها از بین رفته اند؟ به عنوان مثال، آیا درخواست باج دریافت کرده اید یا اطلاعات شما در اینترنت ارسال شده است؟
4. چه اطلاعاتی (درصورت وجود) برای اشخاص غیرمجاز افشا شده، حذف شده یا خراب شده است؟
5. آیا مشتریان شما متوجه مشکلی شده اند؟ آیا آنها می توانند از خدمات شما استفاده کنند؟
6. چه کسی سیستم آسیب دیده را طراحی کرده و چه کسی آن را حفظ می کند؟
7. چه زمانی مشکل ایجاد شد یا برای اولین بار توجه شما را جلب کرد؟
8. دامنه مشکل چیست، چه حوزه هایی از سازمان تحت تأثیر قرار می گیرد؟
9. آیا علائمی مبنی بر اینکه مشکل در داخل سازمان شما رخ داده است یا در خارج از زنجیره تامین شما وجود داشته است؟
10. تأثیر تجاری احتمالی حادثه چیست؟

ازبدترشدن این حادثه جلوگیری کنید

نگاهی به نرم افزار امنیتی خود (مانند هشدارهای آنتی ویروس و لاگها بیندازید تا ببینید آیا میتوانید مشخصات حمله و متعاقباً علت حادثه را شناسایی کنید. اگر قادر به انجام این کار نیستید (اما می دانید کدام دستگاه تحت تأثیر قرار گرفته است) برنامه آنتی ویروس خود را اجرا کنید تا یک اسکن کامل انجام شود و از نتایجی که به شما میدهد یادداشت برداری کنید. اگر چیزی پیدا نشد، از یک برنامه آنتی ویروس جایگزین استفاده کنید.

از اطلاعاتی که جمع آوری کرده اید برای دریافت مشاوره آنلاین از منابع قابل اعتماد مانند وب سایت های پلیس یا امنیتی استفاده کنید. ممکن است بتوانید دستورالعمل‌هایی را در مورد نحوه رفع مشکل در آنجا پیدا کنید، اگرچه قبل از اقدام بر اساس توصیه‌های تأیید نشده باید مراقب باشید.

در صورت قطع اینترنت، در مرحله اول با ISP خود (با استفاده از جزئیاتی که قبلاً در طرح حادثه خود شناسایی کرده اید) تماس بگیرید. اکثر آنها صفحاتی دارند که به در دسترس بودن خدمات مربوط می شوند. ممکن است یاد بگیرید که این قطع به دلیل سقوط درخت(حادثه طبیعی) است نه حمله DDoS. علاوه بر این، اطمینان حاصل کنید که فرآیند تشدید ارائه‌دهنده خود را درک کرده‌اید و می‌دانید که آنها باید بر اساس چه داده‌هایی عمل کنند و بابت چه نوع پشتیبانی هزینه کرده اید.

گام 3:

حادثه را حل کنید

اقدامات در این مرحله به سازمان شما کمک می کند تا در اسرع وقت دوباره راه اندازی شود. همچنین باید تأیید کنید که همه چیز به طور عادی کار می کند و هر مشکلی را برطرف کنید.

اگر فناوری اطلاعات شما به صورت خارجی مدیریت می شود:
با افراد مناسب برای کمک تماس بگیرید با ارائه دهندگان فناوری اطلاعات خارجی خود (که در مرحله 1 شناسایی کرده اید) تماس بگیرید تا به شما در رفع مشکل کمک کنند. این مخاطبین برای رفع مشکل و ایجاد تأثیر بر سازمان شما وجود دارند.

اگر فناوری اطلاعات شما به صورت داخلی مدیریت می شود:
برنامه خود را عملی کنید وقت آن رسیده است که طرح حادثه ای را که در مرحله 1 ساخته اید فعال کنید. بسته به نوع حادثه ای که به آن پاسخ می دهید، ممکن است شامل موارد زیر باشد:

- جایگزینی سخت افزار آلوده
- بازیابی خدمات از طریق پشتیبان گیری
- وصله نرم افزار
- تمیز کردن ماشین آلات آلوده
- تغییر رمز عبور

نکته اقدام: اگر در نظر دارید از خدمات یک مشاور امنیت سایبری استفاده کنید، اقدامات مناسب را انجام دهید تا مطمئن شوید که از سازمان های معتبر استفاده می کنید، تجربه آنها را درک می کنید و می دانید که چگونه پیشنهاد آنها با نیازهای شما و نوع کسب و کار شما مطابقت دارد. مدارک فنی مرتبط یک امتیاز مثبت محسوب می شود. این به شما کمک میکند تا ارائه دهنده ای را انتخاب کنید که مناسب سازمان شما باشد.

گام 4:

حادثه را به ذینفعان گسترده تر گزارش دهید

هنگامی که یک حادثه امنیت سایبری حل و فصل شد، گزارش رسمی اغلب برای ذینفعان داخلی و خارجی مورد نیاز است. حوادث خاصی وجود دارد که شما از نظر قانونی موظف هستید به دفتر کمیسیون اطلاعات گزارش دهید، صرف نظر از اینکه آیا فناوری اطلاعات شما برون سپاری شده

همچنین سایر نهادهای نظارتی که شما به آنها تعلق دارید نیز ممکن است از شما بخواهند که نقض را گزارش دهید.

به مجریان قانون گزارش دهید
همیشه به یاد داشته باشید که حمله سایبری جرم است.
گزارش یک حادثه سایبری را انجام دهید.

بسیاری از اوقات به دلیل شرمندگی شخصی گزارش نمی شوند. با این حال، اگر یک حادثه سایبری علیه شما انجام شده باشد، ممکن است شخص دیگری نیز مرتکب جرم مشابهی شده باشد. هرچه افراد بیشتر گزارش دهند، احتمال دستگیری، متهم شدن و محکومیت عاملان بیشتر است.

همه را در جریان بگذارید

مهم است که کارکنان و مشتریان خود را از هر چیزی که ممکن است آنها را تحت تأثیر قرار دهد (مثلاً اگر اطلاعات شخصی آنها در اثر نقض به خطر افتاده است) مطلع کنید.

نکته اقدام: کارکنان را از هر گونه حادثه در زمانی که متناسب با اثر حادثه است آگاه کنید. بنابراین، اگر شما یک حادثه جزئی را در ساعات کاری تجربه کرده اید، آیا تماس با کارکنان در نیمه شب مناسب است؟ در صورت لزوم، در اسرع وقت از طریق مناسب‌ترین کانال ها با مشتریان خود تماس بگیرید

مشاوره حقوقی را در نظر بگیرید

اگر این حادثه تأثیر قابل توجهی بر کسب و کار و/یا مشتریان شما داشته است، ممکن است بخواهید به دنبال مشاوره حقوقی باشید. اگر بیمه نامه سایبری دارید، آنها می توانند مشاوره های بیشتری را به شما ارائه دهند.

گام 5:

از حادثه درس بگیرید

پس از حادثه، مهم است که:

- آنچه اتفاق افتاده را مرور کنید
- از هر اشتباهی درس بگیرید
- برای کاهش احتمال تکرار آن اقدام کنید

نه تنها بررسی کنترل های فنی خود پس از حادثه مهم است، بلکه فرصتی عالی برای بررسی و اجرای اقدامات آگاهی یا آموزش کارکنان برای کمک به توسعه فرهنگ امنیتی کارکنان است.

اقدامات انجام شده در حین پاسخ را بررسی کنید

اقداماتی را که در طول پاسخ به حادثه مستند کرده اید، جمع آوری و مرور کنید. فهرستی از چیزهایی که به خوبی پیش رفتند و چیزهایی که می‌توانستند از مرحله پاسخگویی بهبود یابند، تهیه کنید.

بازبینی و به‌روزرسانی برنامه حادثه

در صورت لزوم، تغییراتی را در طرح حادثه ای که در مرحله 1 ایجاد کردید، ایجاد کنید تا درس‌های آموخته شده را منعکس کنید.

دفاع خود را تقویت کنید

ریسک خود را دوباره ارزیابی کنید و تغییرات لازم را اعمال کنید.

مثلا،اگر قربانی یک حمله رمز عبور بوده‌اید، ممکن است نیاز داشته باشید که یک خط مشی رمز عبور جدید ایجاد کنید، آموزش جدید ارائه دهید، فضای ذخیره فیزیکی امن برای گذرواژه ها (یا برنامه های مدیریت رمز عبور) برای کارکنان خود فراهم کنید.

شرایط قراردادهای خود را در نظر بگیرید

بسته به میزان موفقیت آمیز بودن پاسخ حادثه، ممکن است لازم باشد یک تصمیم استراتژیک در مورد قراردادهای شخص ثالث خود بگیرید. ممکن است بخواهید موارد زیر را در نظر بگیرید:

- آیا این اتفاق به این معنی است که روش کسب و کار شما باید تغییر کند؟
- اگر در حال حاضر برون سپاری می کنید، آیا پاسخ آنها نیازهای شما را برآورده می کند؟
- اگر آنها نیازهای شما را برآورده نکردند، مجدداً در مورد شرایط قرارداد مذاکره کنید یا آن را لغو کنید و به یک شرکت جدید تغییر دهید.
- آیا به صورت داخلی مهارت هایی داشتید که خودتان این کار را انجام دهید و نیاز به برون سپاری در آینده را نفی کنید؟

با ما در تماس باشید

شرکت "داده پردازی هوشمند کندو" درسال 1402 به منظور ارائه خدمات فناوری اطلاعات و ارتباطات به ویژه در حوزه امنیت اطلاعات تاسیس گردید. هدف اصلی ما ارائه راهکارهای جامع امنیت، جهت حفاظت از اطلاعات و دارایی‌های دیجیتال سازمان‌ها می‌باشد. در تلاش هستیم با خدمات مشاوره، اجرا، پیاده‌سازی و راهبری پروژه‌ها و همچنین ارائه راهکارهای نوآورانه و انعطاف پذیر، به نیازها و انتظارات بازار پاسخ دهیم. ما با توسعه دانش و مهارت کارکنان خود، به افزایش بهره‌وری و ارزش آفرینی می‌پردازیم.

شعار شرکت:
"سپر امنیتی ما، همراهی قدرتمند برای آینده‌ی شما"

www.csdpc.ir
info@csdpc.ir