شهرزاد دانشمند

۱۰ تمرین به منظور ارتباطات پسابحران حملات سایبری

با توجه به مقاله منتشر شده در AT&T امنیت سایبری ۶۲ درصد از تمام سازمان‌های مورد بررسی اعتراف کردند که از نقض سایبری در سال ۲۰۱۵ رنج می‌برند. علاوه بر این، اگر چه ۴۲ درصد گزارش کرده اند که این نقض تأثیر قابل توجهی بر شرکت آن‌ها داشته اما تا به حال، تنها ۳۴ درصد احساس کردند که یک برنامه مؤثر برای پاسخ به این حادثه دارند. ارتباط cyberbreach با تمام گروه‌ها یکی از عناصر مهم است که اغلب در برنامه پاسخ حادثه فاقد یک استراتژی است.

پس از یک حمله سایبری، ۱۰ مورد از بهترین شیوه‌ها برای مدیریت پس از بحران موارد زیر هستند که می‌توانند مفید باشند.

۱ سکوت پس از حمله سایبری مناسب نیست. سازمان‌ها نیاز به ارتباط سریع دارند. درصورت لزوم با یک بیانیه می‌توان اعضای گروه را از وضعیت مطلع کرد و اطلاعات بیشتری را در مورد این اتفاق فراهم خواهد کرد.

۲ تبلیغات معاونت توصیه نمی‌شوند. یک طرح واکنش به‌رخداد مؤثر باید شامل اظهارات تکمیل کننده و آماده‌ای باشد که قبلاً توسط ذی‌نفعان استفاده شده است. بایستی بر این اظهارات تکیه کرد و لاغیر.

۳ ارتباطات را بایستی به صورت آشکار و به طور فنی ارائه داد. اگر پیام ها شفافیت نداشته باشند، مردم ممکن است فکر کنند سازمان چیزی را مخفی کرده است. به همین دلایل از پاسخ دادن به صورت بدون کامنت خودداری کنید.

۴ تمام ارتباطات بایستی هم صدا باشند. این بدان معنی نیست که تنها یک فرد برای رسیدگی به تمام ارتباطات مورد نیاز است. این به این معناست که ارتباطات باید یک پیام سازگار ارائه دهند و استفاده از یک پیام هماهنگ استفاده کنند.

۵ بیشتر بایستی بر روی افراد آسیبدیده تمرکز کرد تا سازمان‌های آسیب دیده.

اطلاع رسانی بایستی به عنوان بخشی از یک استراتژی ارتباط با مشتری، و همچنین به عنوان بخشی از یک طرح واکنش به رخداد در نظر گرفته شود. مشتریان بایستی احساس اهمیت از جانب سازمان‌ها را داشته باشند و هم چنین احساس اهمیت داشتن مشکلات از جانب سازمان را نیز داشته باشند. مردم بایستی نگرانی خود را بدون هیچ چشم داشتی از جانب سازمان ابراز کنند.

۶ از استخدامی‌ها نبایستی توقعی داشت. آن‌ها بایستی در یک سیکل نگه داشته شوند و تمام راهنمایی‌های لازم برای آن‌ها انجام شود.

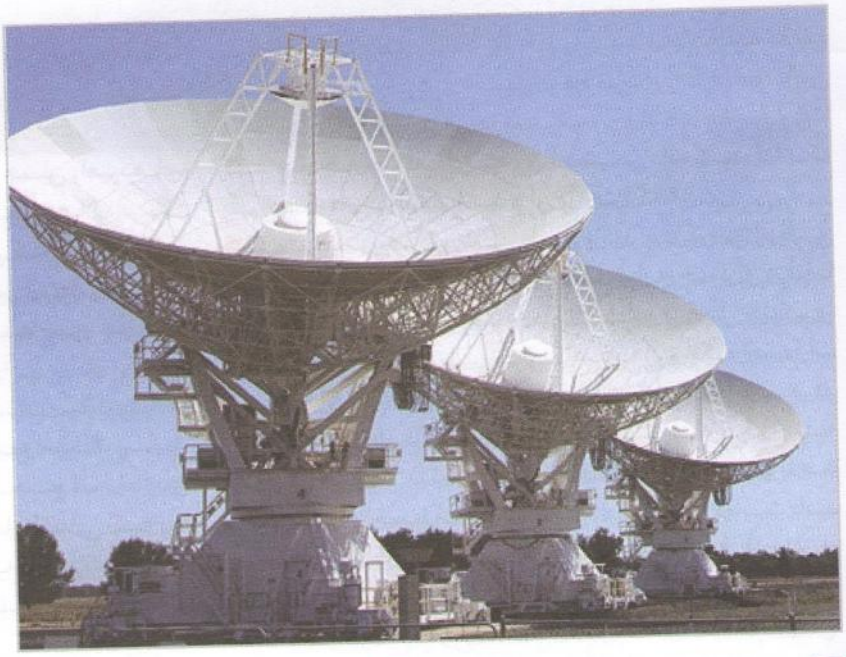
می‌تواند سازماندهی پاسخ به حمله سایبری را سازمان دهد. گزارش‌ها و پیشرفت‌های ناشی از بررسی‌های انجام شده بایستی گزارش شود.

۹ مطمئن بمانید. اگر یک سازمان به کارکنان پاسخ از جانب مشتریان را قول دهد، از دنبال کردن این مسیر مطمئن شوید. اگر از برگزاری یک کنفرانس در یک زمان خاص مطمئن شدید، از حضور داشتن سخنگو در آن مکان مطمئن شوید. اگر به مشتریان اطلاعات بیشتر وعده داده شده است، آن اطلاعات را به‌موقع ارائه دهید. از افتادن مطبوعات و یا مشتریان در ظن این که سازمان چیزی را پنهان می‌کند بپرهیزید.

بحران است.
انجام تمرینات شبیه سازی شده و تحلیل پاسخ از جانب تیم های مختلف می‌تواند می‌تواند وضعیت بهتری را در زمان حمله برای تیم ایجاد کند.

در مورد نویسنده

Rishi Bhargava پایه‌گذار DEMISTO و VP، مسئول فروش یک شرکت در زمینه امنیت شبکه با مأموریت ایجاد شبکه‌های امن‌تر سریع‌تر و سبک‌تر است. قبل از تأسیس Demisto، RISHI معاونت ریاست مدیر نرم‌افزار تعریف مرکز داده گروه در امنیت اینتل بود. علاقه مندان رویایی و فناوری، او مسئول برای ارائه راه حل‌های یکپارچه امنیتی اینتل برای مراکز داده بود. قبل از اینتل، rishi معاون مدیریت محصولات برای مرکز داده و محصولات امنیتی سرور در مک‌آفی و بخشی از امنیت اینتل بود. او در مک‌آفی، راه اندازی محصولات متعدد برای ایجاد رهبری مک‌آفی در ریسک و پذیرش، مجازی سازی و امنیت را بر عهده داشت. RISHI از طریق مصاحبه در سال ۲۰۰۹ به مک‌افی راه پیدا کرد. (Solidcore، شرکت پیوست راه اندازی امنیت). در Solidcore، او مسئول مدیریت محصول و استراتژی بود. به عنوان یکی از اولین کارمندان و اعضای تیم رهبری، او در تعریف استراتژی محصول این شرکت به کسب و کار می‌پرداخت. ریشی دارای انبوهی از اختراعات ثبت شده در زمینه امنیت کامپیوتر دارد. او دارای مدرک کارشناسی در علوم کامپیوتر از مؤسسه فناوری هند، دهلی‌نو و کارشناسی ارشد در رشته علوم کامپیوتر از دانشگاه کالیفرنیای جنوبی، لس‌آنجلس است. RISHI در مورد فناوری‌های جدید و روند صنعت و به‌عنوان یک مشاور فعال به راه اندازی‌های متعدد در زمینه ی سیلیکون و هند پر شور است.



۷ بایستی از ابزار آلات مؤثری به‌منظور ارتباط استفاده کرد. یک بخش در وب‌سایت‌های موجود و یا ایجاد یک وب‌سایت جداگانه که در آن مشتریان و رسانه‌ها می‌توانند اطلاعات فعلی را پیدا کنند در نظر بگیرید. سازمان ممکن است با استفاده از یک سایت اینترانت برای کارکنان، فروشندگان یا دیگران دسترسی به اینترنت را فراهم کند.

۸ نگاهی پیشگیرانه به ارتباطات

۱۰ برنامه های ارتباطی جامعی را درنظر داشته باشید. برنامه‌های ارتباطی باید در دسترس همه دارندگان سهام داخل سازمان باشد. حملات سایبری هم چنان با سرعت بالایی در حال اتفاق افتادن است. نحوه مدیریت ارتباط پس از این حملات تأثیر بسیاری بر افکار عمومی و روابط مشتری‌ها خواهد داشت. این ارتباطات بهترین شیوه برای ایجاد ادراکات مثبت در مورد شرکت در زمان