فصلنامه مدیریت بحران
سال هفتم، شماره‌ی ۲۵، پاییز ۹٤

شناخت و مدیریت بحران‌ها در دنیای مجازی

نویسندگان: سارا کوور- میزرا و ماناوندرا میزرا*
مترجم: دکتر قدرت حاجی رستملو

تاریخ دریافت مقاله ۹٤/۰۵/۱۹
تاریخ پذیرش مقاله ۹٤/۰٦/۲۰

صفحات: ۱٤۱-۱۷۱

چکیده

گسترش استفاده از اینترنت به عنوان وسیله انجام فعالیت‌های اقتصادی، موجب شده است ارزیابی و شناخت مخاطرات مربوط به محیط‌های مجازی و نحوه آمادگی سازمان‌ها برای مدیریت این تهدیدات از اهمیت فراوانی برخوردار گردد. هدف اصلی مقاله حاضر پاسخ دادن به این سؤال است که چرا محیط‌های مجازی سازمان‌ها را آسیب‌پذیر کرده است. برای پاسخ دادن به این سوال، ابتدا تهدیدات مربوط به فضای مجازی معرفی می‌شود و سپس اشکال ممکن این تهدیدات، ارتباط آنها با بحران‌های سنتی، و مضامین آنها برای مدیریت بحران مورد بررسی قرار می‌گیرد. در آخر، بعد از ارائه راهبردهای مدیریت بحران، پیشنهاد-اتی برای پژوهش‌های آینده ارائه می‌گردد.

کلیدواژه‌ها: مدیریت بحران، دنیای مجازی، بحران‌های اینترنتی، بحران‌های سنتی

---

* Sarah Kovoor-Misra and Manavendra Misra

مقدمه

با توجه به کاربرد گسترده فن‌آوری‌های رایانه‌ای در انجام فعالیت‌های اقتصادی، شناخت تهدیدات ذاتی مربوط به محیط‌های مجازی از اهمیت زیادی برخوردار است. مطالعات انجام پذیرفته در حوزه مدیریت بحران، اشکال مجازی بحران و مضامین آنها برای مدیریت بحران را به اندازه کافی مورد توجه قرار نداده‌اند. مقاله حاضر به چند سؤال مربوط به این موضوع پاسخ می‌دهد: چرا محیط‌های مجازی سازمان‌ها را آسیب‌پذیر می‌کند؟ اشکال مختلف بحران‌های احتمالی تهدید کننده سازمان‌ها کدام‌ها هستند؟ مدیریت بحران چه راهبردهایی را در این زمینه ارائه می‌کند؟ و چه پیشنهاداتی برای پژوهش‌های آینده در این زمینه مطرح است؟

بدنبال فجایع بوپال و چلنجر در دهه ۱۹۸۰، ما شاهد توجه فزآینده محققین به موضوع مدیریت بحران بودیم. بحران به یک حادثه، وضعیت و روندی اطلاق می‌شود که بقاء و یا اهداف یک سازمان را به مخاطره می‌اندازد (نیسترم و استارباک[1]، ۱۹۸٤). محققین اشارات روشنگرانه‌ای را در خصوص علل و مصادیق بحران یادآور شده و راهبردهایی را برای مدیریت بحران توصیه کرده‌اند (پیرسون و میترف[2]، ۱۹۹۳).

در طول ۲۰ سال گذشته، ما همچنین شاهد تغییرات مهمی در فضای فعالیت‌های اقتصادی مربوط به مدیریت بحران بوده‌ایم. اینترنت ارتباطات مربوط به فعالیت‌های اقتصادی و ابعاد مختلف آنها را دگرگون ساخته و مخاطرات جدیدی شکل پیدا کرده است. در فوریه سال ۲۰۰۰، یک هکر چهارده ساله از مونترال کانادا با نام «مافیابوی»[3]، برخی از مهمترین وب سایت‌ها را با هدف جلوگیری از فعالیت آنها مورد حمله قرار داد. او به تنهایی وب‌سایت شرکت‌های مهمی مثل یاهو،

1- Nystrom and Starbuck
2- Pearson and Mitroff
3- MafiaBoy

آمازن، ایی بی[1]، بای‌دات‌کام[2]، ایی‌ترید[3]، دیتک آنلاین[4]، و سی اِن اِن را از کار انداخت. گفته می‌شود این شرکت‌ها در اثر این حمله متحمل بیش از ۱/۷ میلیارد دلار خسارت شدند.(۱) تقریباً در همین زمان، هکر دیگری بنام «کورادور»[5] مدعی بود که حداقل به هشت سایت تجاری دسترسی غیر قانونی پیدا کرده و بیش از ۲۳۰۰۰ هزار شماره کارت اعتباری را بسرقت برده است. بدنبال این ماجرا، وی شماره‌های فوق را در وب سایت خود به نمایش گذاشته بود (بورلند[6]، ۲۰۰۰).

این مخاطرات جدید نه‌تنها سازمان‌های مجازی محض را تهدید می‌کنند، بلکه امکان حمله به سازمان‌های سنتی مرتبط با شبکه جهانی را مطرح می‌کنند. امروزه، بسیاری از سازمان‌های سنتی مانند بانک‌ها، شرکت‌های پخش، و مؤسسات آموزشی فعالیت‌های اینترنتی را دنبال می‌کنند. با گسترش استفاده از اینترنت به عنوان وسیله انجام فعالیت‌های اقتصادی، ارزیابی و شناخت مخاطرات مربوط به محیط‌های مجازی و نحوه آمادگی سازمان‌ها برای مدیریت این تهدیدات اهمیت فراوانی پیدا کرده است.

اما همگام با این تغییرات، فعالیت‌های پژوهشی کافی صورت نگرفته است، و برای شناخت تهدیدات مربوط به فضای مجازی، اشکال ممکن این تهدیدات، ارتباط آنها با بحران‌های سنتی، و مضامین آنها برای مدیریت بحران توجه کافی مبذول نشده است. مقاله حاضر در صدد است به بخشی از این نیازهای پژوهشی بپردازد، و در این ارتباط سعی شده است به این سؤال پاسخ داده شود که چرا محیط‌های مجازی سازمان‌ها را آسیب‌پذیر می‌کنند. همچنین، اشکال مختلف بحران‌های اینترنتی اتفاق افتاده و جایگاه آنها در تقسیم‌بندی‌های کنونی بحران‌ها در اینجا مورد بررسی قرار می‌گیرد. در آخر، بعد از طرح راهبردهای مدیریت بحران، پیشنهاداتی برای پژوهش‌های آینده ارائه می‌گردد.

1- eBay
2- Buy.com
3- E*Trade
4- Datek Online
5- Curador
6- Borland

تهدیدات محیط‌های مجازی

سازمان‌ها برای انجام فعالیت‌های اقتصادی، بشکل‌های مختلفی از محیط‌های مجازی استفاده می‌کنند. برخی سازمان‌ها مانند آمازن دات کام عرضه کالاها و خدمات را به طور کامل با استفاده از اینترت انجام می‌دهند. برخی دیگر مانند بانک‌ها و فروشگاه‌ها شیوه سنتی فعالیت‌های خود را دنبال می‌کنند، ولی در عین حال از اینترنت نیز برای عرضه کالا و خدمات استفاده می‌کنند. با این حال، بیشتر سازمان‌ها برای اطلاع رسانی و انجام فعالیت‌های عادی روزانه از اینترنت استفاده می‌کنند. در این بخش، برخی از ویژگی‌های محیط‌های مجازی بحران‌ساز برای سازمان‌ها مورد بحث قرار می‌گیرد.

دسترسی آسان، شمشیر دو لبه

شبکه جهانی اینترنت امکان دسترسی به وب سایت شرکت‌ها را بطور شبانه-روزی برای کاربران فراهم می‌کند. بنابراین، فاصله جغرافیایی و زمان موانع مهمی برای دسترسی به مشتریان بحساب نمی‌آیند. اما همین ویژگی که امکان دسترسی به مخاطبین جهانی را فراهم می‌کند، در عین حال می‌تواند یک حمله خصمانه را از فاصله جغرافیایی دور و در هر نقطه زمانی امکان‌پذیر سازد. برای مثال، حملات مافیابوی که قبلاً مورد اشاره قرار گرفت، در کانادا طراحی شده بود ولی تعدادی از شرکت‌ها را در آمریکا بشدت تحت تأثیر خود قرار داد. در مورد دیگری، اول ماه مه سال ۲۰۰۱ شاهد چندین حمله از سوی فعالان چینی به تعدادی از سایت‌های دولتی آمریکا بود که برای اعتراض به دست داشتن آمریکا در بحران ناشی از سانحه هواپیمای جاسوسی صورت پذیرفته بود. بعلاوه، ماهیت فرامرزی اینگونه حوادث تعقیب مجرمین را برای مسئولین کشورها مشکل می‌سازد. برای مثال، به دلیل عدم وجود قوانین ناظر بر عمالکرد هکرها در فیلیپین، تولید کننده

ویروس«لاو باق»[1] نتوانست تحت تعقیب قرار گیرد.[۲] این درحالی است که برای متوقف ساختن فعالیت نمایندگی‌های یک شرکت غیر مجازی، کار سازماندهی قابل توجهی مورد نیاز است تا افراد لازم بتوانند در موقعیت‌های مربوطه حاضر شوند. بنابراین، برای عملی کردن تهدیدات فیزیکی علیه سازمان‌های غیر مجازی، بعد جغرافیایی یک مانع به حساب می‌آید. اما در ارتباط با سازمان‌های اینترنتی چنین مانعی مطرح نیست.

عملیات متمرکز

آنچه که آسیب‌پذیری سازمان‌های مجازی را تشدید می‌کند، تمرکز عملیات‌های اینترنتی است. وب سایت‌ها از سرورهایی استفاده می‌کنند که در یک مرکز داده متمرکز هستند و این موضوع نقطه ضعفی را ایجاد می‌کند که ممکن است ناخواسته و یا مغرضانه مورد بهره‌برداری قرار گیرد. حتی آن دسته از شرکت‌هایی که می‌توانند مراکز داده متعددی داشته باشند، نوعاً بیش از چند مرکز داده ندارند. این بدان معنی است که مثلاً هرگونه قطع برق (خواه به شکل عادی صورت پذیرد و یا در اثر حملات مغرضانه) می‌تواند مانع فعالیت‌های اینترنتی شرکت گردد.

معماری اینترنت

علاوه بر عملیات‌های متمرکز، نوع معماری اینترنت نیز بسیاری از سازمان‌های اینترنتی را آسیب‌پذیر کرده است. اینترنت به عنوان ابزاری برای همکاری‌های پژوهشی طراحی شده است، و به همین دلیل سازوکارهای امنیتی کافی در این سیستم در نظر گرفته نشده است. برخلاف شبکه مخابراتی که در آن دسترسی به عوامل کنترل شبکه برای کاربران فوق‌العاده مشکل است، سازوکارهای انتقال و کنترل اینترنت همزمان بر روی یک شبکه قرار دارند. همه ابزارهای کنترلی مانند

1- Love Bug

مسیریاب‌ها و سویچ‌ها در دسترس یک پروتکل اینترنتی (IP) قرار دارند که از همان سازوکارهای مورد استفاده کاربران برای دسترسی به سرورهای اینترنتی بهره-برداری می‌کند. و این بدان معنی است که یک هکر می‌تواند به زیرساخت‌های اینترنت دسترسی پیدا کرده و باعث اختلال گردد و این هم به نوبه موجب جلوگیری از دسترسی به برخی وب سایت‌ها می‌شود.

حجم بالای اطلاعات مشتری

برخلاف یک فروشگاه سنتی که مشتری می‌تواند بی نام و نشان از آن خرید کند، ماهیت تجارت الکترونیکی باعث گردیده است شرکت‌های اینترنتی حجم انبوهی از اطلاعات مربوط به مشتری از قبیل اسم، شماره کارت اعتباری، و آدرس را جمع‌آوری کنند. این حجم انبوه اطلاعات که برای خرابکاران احتمالی در هر نقطه دنیا نیز قابل دسترسی است، یک نوع آسیب‌پذیری در مقابل بحران‌ها بوجود می‌آورد. در ژانویه سال ۲۰۰۰، هکری که خود را «ماکسوس»[1] معرفی می‌کرد، مدعی بود که شماره ۳۵۰۰۰۰ کارت اعتباری را از فرشگاه اینترنتی سی‌دی-یونیورس[2] به سرقت برده است و در مقابل خواهان ۱۰۰۰۰۰ دلار از شرکت مربوطه بود (بورلند، ۲۰۰۰). از دست رفتن اطلاعات حساس مشتریان، این سازمان‌ها را در معرض زیان‌های اقتصادی، از دست رفتن اعتبار، و مسئولیت‌های حقوقی احتمالی قرار می‌دهد.

فعالیت شبانه‌روزی در هفت روز هفته

آنچه که به این مشکلات دامن می‌زند این واقعیت است که سازمان‌های اینترنتی برای رفع مشکلات بوجود آمده در سیستم‌های خود فرصت زیادی در اختیار

1- Maxus
2- CD Universe

ندارند.آنها در هفت روز هفته بطور شبانه‌روزی به فعالیت مشغول هستند. در نتیجه، رفع مشکلات به سختی انجام می‌پذیرد، زیرا این کار غالباً همزمان با انجام فعالیت-های جاری صورت می‌گیرد. این در حالی است که شرکت‌های سنتی از فرصت کافی برای پرداختن به مشکلات خود در ساعات تعطیلی برخوردارند.

در معرض دید بودن

و آنچه که همه این مسائل را می‌تواند تحت‌الشعاع قرار دهد این واقعیت است که مسائل مربوط به عملکرد سازمان‌های اینترنتی در معرض دید همگان قرار دارد. برای مثال، هر مراجعه کننده به سایتی، از عدم فعالیت آن مطلع می‌شود. بعلاوه، فضای تبلیغاتی حاکم بر اینترنت باعث پوشش رسانه‌ایی بیش از حد سایت‌ها می-گردد. این موضوع موجب شده است این گونه شرکت‌ها مورد هدف حملات هکرهای جویای توجه و شهرت قرار گیرند. در معرض دید همگان بودن می‌تواند نگرش سرمایه‌گذاران را نیز تحت تأثیر قرار دهد. یک حادثه جدی می‌تواند ارزش سهام اینگونه شرکت‌ها را بشدت کاهش دهد. مثلاً در ژانویه سال ۱۹۹۹، قطعی برق شرکت ایی‌بی موجب شد سهام آن ۲۰ درصد کاهش پیدا کند.(۳)

پخش سریع اطلاعات و مشتریانی که پیوسته در ارتباط هستند

اینترنت به عنوان یک رسانه، امکان پخش سریع اطلاعات و شایعات را فراهم می‌آورد. از طریق نامه‌های الکترونیکی همگانی، گروه‌های گفتگوی اینترنتی، و وب سایت‌های متقلب شایعات بسرعت پخش و ماندگار می‌شوند. برای مثال، شرکت کاریبوکافی[1] مجبور بود خود را از یک شایعه دو ساله مبنی بر داشتن ارتباط با گروه‌های تروریست خلاص بکند. این شایعه باعث شده بود فروش آنها در جوامع یهودیان کاهش پیدا کند. شرکت پراکتور وگنبل[2] نیز مجبور بود با شایعه‌ایی مبنی

1- Caribou Coffee
2- Procter and Gamble

برداشتن ارتباط با شیطان مقابله کند. (اشملتزر[1]، ۲۰۰٤).

به علاوه، با گسترش ارتباطات مشتریان سازمان‌های اینترنتی از طریق ایمیل و گروه‌های گفتگو و بحث، نارضایتی می‌تواند بسرعت در میان آنها گسترش پیدا کند. سازماندهی یک تحریم از طرف توده مردم بر علیه یک فروشگاه زنجیره‌ایی سنتی مستلزم توان اجرایی، زمان و منابع قابل توجهی است. اما ارتباط نزدیک مشتریان سازمان‌های اینترنتی افراد ناراضی را قادر می‌سازد با اعمال فشار سازمان را مجبور به تغییر رفتار بکنند. برای مثال، در سال ۱۹۹۹، شرکت ایی‌تویز[2] بر علیه گروهی از هنرمندان که از اسم این شرکت استفاده کرده بودند، اقامه دعوی کرد. این افراد که فاقد منابع یک سازمان بزرگ بودند، از طریق اینترنت به یک ضد حمله‌ایی به نام توی‌وار[3] دست زدند. این گروه کوچک با استفاده از ایمیل، گروه‌های بحث، و وب سایت‌ها توانست هزاران نفر از فعالان کشورهای مختلف را در یک تحریم و مبارزه هماهنگ بر علیه ایی‌تویز بسیج کند. سرانجام، ایی‌تویز مجبور گردید اقامه دعوی را رها کند.(٤) علت موفقیت توی‌وار این بود که تعداد زیادی از فعالان از طریق اینترنت وارد صحنه شده بودند.

هکرهای با انگیزه

بر خلاف دیگر صنایع، در حوزه اینترنت مجموعه‌ایی از هکرها وجود دارند که برای پیدا کردن اشکالات در فن‌آوری سازمان‌های اینترنتی از زرنگی و انگیزه کافی برخوردار هستند. غالباً انگیزه این هکرها نیاز به جلب توجه و کسب شهرت است و یا اینکه صرفاً بدنبال این هستند که ثابت کنند می‌توانند یک سیستم دارای فن‌آوری خیلی پیشرفته را از کار بیاندازند. دسترسی آسان این افراد را قادر می‌سازد با از کار انداختن یک سایت، تخصص خود را به رخ دیگران بکشند. بر خلاف

1- Schmeltzer
2- eToys
3- Toywar

دنیای واقعی که در آن برای وارد آوردن خسارت بر کسی یا جایی یک گروه سازمان یافته مورد نیاز است، این هکرها به تنهایی می‌توانند در دنیای مجازی خسارات عمده‌ایی را ببار آورند. بیشتر فروشگاه‌ها در دنیای غیر مجازی مبلغ کمی را برای جلوگیری از سرقت یا کاهش فروش هزینه می‌کنند، اما در دنیای مجازی هکرها می‌توانند به تنهایی شرکتی را کاملاً به تعطیلی بکشند. ماجراهای مافیابوی، کورادور و ماکسوس مصادیق این نوع مخاطرات هستند.

به طور خلاصه می‌توان گفت دسترسی آسان، تمرکز فعالیت‌ها، نبود امنیت کافی در ساختار اینترنت، فعالیت شبانه‌روزی در تمام روزهای هفته، در معرض دید بودن، پخش سریع شایعات، ارتباط نزدیک کاربران، و هکرهای با انگیزه همه و همه سازمان‌های اینترنتی را در معرض آسیب‌پذیری‌های بحران‌ساز قرار می‌دهند. در بخش بعد، اشکال مختلف بحران‌های تهدید کننده سازمان‌های مرتبط با اینترنت مورد بررسی قرار گرفته و بحران‌های ویژه سازمان‌های اینترنتی و بحران‌های مشترک بین سازمان‌های اینترنتی و سازمان‌های سنتی بررسی می‌شود.

اشکال بحران‌های اینترنتی

ترکیب ضعف‌های فردی و سازمانی یا تغییرات در محیط سازمانی که سازمان را وادار به عکس‌العمل می‌نمایند ممکن است باعث بروز بحران شوند (همبریک و دوعاونی[1]، ۱۹۸۸؛ کوور- میزرا، کلیر و بتن‌هوسن[2]، ۲۰۰۱؛ پاچنت و میترف[3]، ۱۹۹۲؛ شیرواستوا[4]، ۱۹۷۸؛ ترنر[5]، ۱۹۷٦). برای مثال، علت برخی از بحران‌های ناشی از توقف فعالیت سازمان‌های مجازی، عدم برخورداری آنها از فن‌آوری‌های لازم برای تفکیک درخواست‌های مشتریان عادی و متقلب و افراد دارای مقاصد

1- Hambrick and D'Aveni
2- Kovoo-Misra, Clair and Bettenhausen
3- Pauchant and Mitroff
4- Shirvastava
5- Turner

خصمانه می‌باشد. در این ارتباط می‌توان به از بین رفتن سازمان‌های اینترنتی زیادی مانند اموییپی‌کام[1]، گاردن‌کام[2]، و وب‌ون‌کام[3] اشاره کرد که به علت عدم توانایی رقابت در فضای جدید به این عاقبت دچار شدند.

همچنین، بحران‌ها اغلب دارای ابعاد مختلف می‌باشند و دیده می‌شود که در یک شرایط واحد چندین بحران مطرح است، به طوری که یک بحران منجر به بحران‌های دیگر می‌شود (کوور- میزرا، ۱۹۹۵؛ پیرسون و میترف، ۱۹۹۳). برای مثال، در بحران ناپستر[4] که این سازمان از طرف سازمانی دیگر تحت پیگرد حقوقی قرار داشت، ادامه حیات اقتصادی این سازمان و اعتبار آن در خطر بود، و آنها با مسائل حقوقی بعدی دست به گریبان بوند. هنگامی که هکرها به سازمانی حمله می‌کنند، سازمان مجبور است از فن‌آوری و اعتبار خود محافظت کرده و زیان‌های اقتصادی احتمالی را به حداقل برساند. بنابراین، یک سازمان اغلب با انواع بحران‌های مهم مواجه است.

بحران‌ها ممکن است اشکال مختلفی پیدا کنند. محققین حوزه مدیریت بحران نیز بحران‌های فراروی سازمان‌های سنتی را به شکل‌های مختلف تقسیم‌بندی کرده‌اند (فینک[5]، ۱۹۸٦؛ پیرسون و میترف، ۱۹۹۳). برای مثال، بحران‌ها را می‌توان از یک سو بر اساس ماهیت فنی- اقتصادی یا انسانی و اجتماعی آنها، و از سوی دیگر بر اساس ماهیت شدید یا عادی آنها تقسیم‌بندی کرد (پیرسون و میترف، ۱۹۹۳). در شیوه دیگر، بخش بحران‌خیز و بخش متأثر از بحران سازمان مبنای تقسیم‌بندی قرار می‌گیرد (کوور- میزرا، ۱۹۹۵). بنابراین، سازمان‌ها ممکن است با بحران‌های فنی، اقتصادی، انسانی و اجتماعی، و سیاسی مواجه شوند.

همین شیوه‌های تقسیم‌بندی را می‌توان برای دسته‌بندی بحران‌های اینترنتی نیز

1- Mvp.com
2- Garden.com
3- WebVan.com
4- Napster
5- Fink

استفاده کرد. اما مصادیق بحران‌های مربوط به هر دسته ممکن است نسبت به بحران‌های فراروی سازمان‌های سنتی متفاوت باشند. در جدول (۱) از همین شیوه‌ها برای معرفی بحران‌های عمومی مربوط به سازمان‌های اینترنتی و سازمان‌های سنتی و همچنین بحران‌های خاص سازمان‌های اینترنتی استفاده شده است.

جدول ۱: برخی از بحران‌های مربوط به سازمان‌های اینترنتی

دسته‌بندی	بحران‌های عمومی (مربوط به سازمان‌های اینترنتی و سازمان‌های سنتی)	بحران‌های اینترنتی (خاص سازمان‌های اینترنتی)
۱. بحران‌های فنی (این بحران‌ها ممکن است بدلیل عدم کارکرد درست فن‌آوری بروز کنند و یا ممکن است بر فن‌آوری تأثیرگذار باشند)	از دست رفتن اطلاعات	خرابی وب سایت
۲. بحران‌های انسانی و اجتماعی (این بحران‌ها ممکن است به دلیل سوء عملکرد افراد بروز کنند و یا ممکن است بر سلامت روانی و جسمی آنها تأثیرگذار باشند)	خشونت در محل کار اعتصابات تهدیدات بمب‌گذاری	حملات سرکاری اینترنتی باجگیری اینترنتی
۳. بحران‌های روابط عمومی(این بحران‌ها اعتبار سازمان و روابط آن با ذینفعان خارجی را تحت تأثیر قرار می‌دهند)	اشتهار منفی	اشتهار منفی ناشی از بحران‌های خاص اینترنتی
٤. بحران‌های حقوقی(این بحران‌ها بدلیل نقض قوانین بروز کنند)	نقض قوانین مربوطه	عدم رعایت حقوق انحصاری آثار و عدم رعایت حریم خصوصی (این نوع بحران بطور خاص مربوط به سازمان‌های اینترنتی نیست، اما اخیراً اهمیت زیادی پیدا کرده است)

در اینجا، پنج نو بحرانی که اخیراً برای سازمان‌های اینترنتی اهمیت خیلی زیادی پیدا کرده است، معرفی می‌شود: خرابی وب سایت، حملات سرکاری اینترنتی[1]، باج‌خواهی و خرابکاری مجازی، تحریم‌های مجازی، و مسائل مربوط به حقوق انحصاری آثار و حریم خصوصی. همچنین، چگونگی شکل‌گیری بحران‌های دیگر به واسطه این بحران‌ها در اینجا تشریح می‌شود. دامنه و تأثیر شرایط فوق مشخص می‌کند که آیا آنها در حال نزدیک شدن به آستانه بحران هستند یا نه. همان طور که گفته شد، بحران به شرایطی اطلاق می‌شود که ادامه حیات و اهداف سازمان را به مخاطره بیاندازد؛ از این رو، اگر این شرایط برای سازمان‌ها هزینه‌های اقتصادی، انسانی، اجتماعی یا حیثیتی بدنبال داشته باشند، می‌توان آنها را بحران نامید.

خرابی وب سایت

خرابی وب سایت یک مسئله فنی است که در هسته فنی سازمان‌های اینترنتی بروز می‌کند. این مشکل ممکن است بدلایلی از قبیل اشکالات نرم‌افزای یا طراحی ضعیف سیستم ایجاد شود. وب سایت سازمان‌های اینترنتی در مقابل حجم بالای ترافیک و مشکلات مربوط به شبکه‌های خارج از خود نیز آسیب‌پذیر هستند. ترافیک اینترنتی سازمان‌های آنلاین دوره‌ایی بوده و اغلب غیر قابل پیش‌بینی می‌باشند. در طول روز و همین‌طور در طول سال، دوره‌هایی با نقطه اوج کاملاً مشخص وجود دارند. از آنجایی که تعدادی از شرکت‌های تجارت الکترونیکی در بازار هدایا فعال هستند، نقطه اوج فعالیت آنها در مناسبت‌های هدیه‌دهی می‌باشد. برای مثال، در طول ٦ هفته قبل از کریسمس، ترافیک سایت‌های اسباب‌بازی ده برابر می‌شود. در سال ۱۹۹۹، به دلیل عدم پیش‌بینی درست ترافیک کار، تقریباً همه

۱- این نوعی حمله برنامه‌ریزی شده است که برای ایجاد مزاحمت در دسترسی به وب سایت انجام می‌پذیرد. در این نوع حمله، انبوهی از درخواست به وب سایت ارسال می‌شود که امکان پاسخگویی به آنها وجود ندارد. به این ترتیب، سرویس دهنده چنان مشغول پاسخگویی به این درخواست‌ها می‌شود که از پاسخگویی به مشتریان واقعی خود باز می‌ماند.

سایت‌های تجارت الکترونیکی دچار مشکل شدند. مثلاً سایت تویزروس‌کام[1] به دلیل ارسال کوپن‌های تخفیف شرکت از طرف مشتریان با حجم فوق‌العاده انبوهی از مراجعات مواجه گردید. بسیاری از شرکت‌ها بناچار بخشی از مراجعات را بی‌پاسخ گذاشتند که نتیجتاً تعداد زیادی از مشتریان نتوانستند به سایت مورد نظر دسترسی پیدا کنند.(۵) در نتیجه این مشکلات، این صنعت در سال ۲۰۰۰ به پختگی بیشتری رسید. شرکت‌های خدماتی مانند مرکوری اینتراکتیو[2] برای جوبگویی به ترافیک واقعی، فن‌آوری‌های مناسبی را طراحی کردند، به طوری که سایت‌های تجارت الکترونیکی توانستند خود را برای نقطه اوج فعالیت‌های فصل بعد بهتر آماده کنند.

به علاوه، مشکلات وب سایت سازمان‌های اینترنتی ممکن است به دلیل مسائلی بروز کند که ریشه در شبکه‌های بیرونی دارند و مانع دسترسی مشتریان به این سایت‌ها می‌شوند. برای مثال، در مارس سال ۲۰۰۱، خدمات پیشرفته یاهو (ارسال پیام آنی، پست الکترونیکی، مای یاهو) به دلیل وجود مشکل در یک مسیریاب جهانی در شهر دنور[3] به مدت یک روز برای بخش عمده مخاطبین غیر قابل دسترس بود.

قطع فعالیت سایت‌های سازمان‌های مهم اینترنتی موجب جلب توجه گسترده رسانه‌ها می‌گردد. بنابراین، این سازمان‌ها مجبور هستند به مسائل روابط عمومی مربوطه نیز پرداخته و اعتماد مشتریان خود را حفظ کنند. بعلاوه، در این شرایط، عدم دسترسی مشتریان به وب سایت باعث از دست دادن درآمد شده و همان طور که تجربه شرکت ایی‌بی نشان داد در برخی موارد این مسئله موجب می‌شود اعتبار اقتصادی یک شرکت به طور قابل توجهی آسیب ببیند.

1- Toysrus.com
2- Mercury Interactive
3- Denver

حملات سرکاری اینترنتی

حملات سرکاری به سازمان‌های اینترنتی نمونه‌ایی از بحران‌های انسانی و اجتماعی است. این بحران‌ها توسط افراد دارای مقاصد خصمانه انجام شده و موجب از کار افتادن وب سایت شرکت‌ها می‌گردد. همان طور که قبلاً گفته شد دسترسی آسان به سازمان‌های اینترنتی حمله به سرورهای آنها را از سوی افراد مغرض نسبتاً تسهیل کرده است. تشخیص درخواست‌های واقعی از موارد تقلبی برای وب سایت کار مشکلی است. بنابراین، مشتریان عادی به هنگام مراجعه به سایت می‌بینند که سرعت سیستم پایین آمده و نهایتاً سرورها از کار می‌افتند. این موضوع «پاشنه آشیل» شرکت‌های اینترنتی است و وجود نقطه ضعف در هر بخشی از معماری سیستم‌ها، آنها را در مقابل مشکلات اتفاقی و یا حملات خصمانه آسیب‌پذیر می‌کند.

در ماه ژوئن سال ۲۰۰٤، شرکت آکامای[1] مورد حمله قرار گرفت. از آنجایی که سرورهای این شرکت محتوای وب سایت‌های شرکت‌های مایکروسافت، گوگل، و یاهو را تأمین می‌کرد، در اثر این حمله سرعت وب سایت‌های این شرکت‌ها به شدت پایین آمد (آسوشیتد پرس، ۲۰۰٤). به دلیل آشکار شدن آسیب‌پذیری‌های فنی سازمان‌ها، به دنبال حملات اینترنتی ضعف‌های وب سایت‌ها و مسائل روابط عمومی مربوطه بروز می‌کند. همچنین، در صورت عدم دسترسی مشتریان به وب سایت، سازمان‌های اینترنتی متحمل ضرر مالی نیز می‌شوند. در این گونه موارد، سازمان‌ها مجبورند برای تعقیب هکرها با سازمان‌های انتظامی مانند اف‌بی‌آی همکاری کنند.

باجگیری و خرابکاری اینترنتی توسط هکرها

این یک نوع دیگر از بحران‌های انسانی و اجتماعی است که در آن خرابکاران با

1- Akamai

پیدا کردن منافذ امنیتی در نرم‌افزارهای شرکت‌ها، اطلاعات مراکز داده آنها را به سرقت می‌برند. در سال ۲۰۰۱، اف‌بی‌آی به شرکت‌های تجارت الکترونیکی در خصوص یک نوع اخاذی هشدار داد که طی آن هکرها وارد مراکز داده مربوط به کارت‌های اعتباری می‌شدند. آنها سپس با مدیریت شرکت تماس می‌گرفتند و در مقابل عدم سوء استفاده از کارت‌ها و عدم افشای ورود خود به سیستم مربوطه مبالغ هنگفتی مطالبه می‌کردند.(۶)

در یک وضعیت بحرانی دیگر، هکرها وارد سیستم شده و اطلاعات مربوط به مشتریان را به سرقت می‌برند. در دسامبر سال ۲۰۰۳، هکرها به مراکز داده مربوط به مشتریان شرکت اِقهد[1] نفوذ کرده و به اطلاعات مربوط به حدود ۳/۷ میلیون مشتری دسترسی پیدا کردند. در سپتامبر سال ۲۰۰۰، در یک حمله مشابه یک هکر توانست شماره‌های حدود ۱۵۷۰۰ کارت اعتباری را از سایت شرکت وسترن یونین به سرقت ببرد. همچنین، اف‌بی‌آی یک تبعه روسی را شناسایی کرد که بیش از ۳۰۰۰۰۰ شماره کارت اعتباری را از شرکت سی‌دی یونیورس به عنوان فروشنده اینترنتی موسیقی بسرقت برده بود (لموس و چارنی[2]، ۲۰۰۰؛ موصیل[3]، ۲۰۰۰).

چنین اتفاقاتی باعث می‌شود حیثیت شرکت‌ها دچار خدشه شده و در نتیجه مشتریان نتوانند در خصوص حفظ اطلاعات محرمانه خود توسط شرکت‌ها به آنها اعتماد کنند. در این شرایط، مشتریان ممکن است برخی شرکت‌ها را ترک کرده و بدنبال شرکت‌های مطمئن‌تر بروند.

تحریم اینترنتی محصولات و خدمات

تحریم اینترنتی محصولات و خدماتیکی از مصادیق بحران‌های روابط عمومی است که شرکت‌های اینترنتی ممکن است با آن مواجه شوند. اینگونه بحران‌ها

1- Egghead.com
2- Lemos and Charny
3- Musil

باعث مخدوش شدن حیثیت شرکت‌ها می‌گردد. سازمان‌های اینترنتی بطور خاصی در برابر این نوح بحران‌ها آسیب‌پذیر هستند، زیرا مخاطبان آنها ارتباط نزدیکی با یکدیگر دارند و می‌توانند بسرعت واژه تحریم را پخش کرده و یک سایت را به تعطیلی بکشانند. بحثی که قبلاً در ارتباط با شرکت ایی‌تویز مطرح گردید، آسیب‌پذیری سازمان‌های اینترنتی را در برابر چنین اقداماتی به وضوح نشان می‌دهد. اگرچه حوادث خیلی گسترده‌ایی از این نوع تا حال مطرح نبوده است، اما شرکت‌های سنتی که در اینترنت حضور دارند ممکن است مورد هدف افرادی قرار گیرند که در صدد مبارزه با شرکت‌های بزرگ هستند. دسترسی آسان به اطلاعات و در معرض دید بودن فعالیت‌های اینگونه شرکت‌ها آنها را به اهداف مطلوبی برای افراد مربوطه تبدیل می‌کند. شکل دیگر این نوع بحران زمانی مطرح می‌شود که از اینترنت برای سازماندهی تحریم‌ها و اعتراضات استفاده می‌شود. شرکت‌های بزرگی که سیاست‌ها و فعالیت‌های اقتصادی آنها برای برخی گروه‌ها مسئله‌ساز است، اغلب مورد هدف چنین حرکت‌هایی هستند. برای مثال، وب‌سایت‌های زیادی وجود دارند که امکان بحث و سازماندهی فعالیت‌ها را بر علیه شرکت وال‌مارت[1] (به سایت http://www. Walmartwatch.com مراجعه کنید) و مایکرو سافت (سایت جنبش تحریم مایکرو سافت، http://www.msboycott.com، فهرست بیش از ۱۶۰ سایت و گردهمایی اینترنتی را ارائه کرده است) فراهم می‌کنند. برخی از سایت‌های ضد وال‌مارت برای مبارزه جدی با فروشگاه‌های بزرگ وال‌مارت در جاهایی مانند اینگل‌وود و کالیفرنیا مورد استفاده قرار گرفته‌اند. اینگونه اقدامات تحریمی حیثیت شرکت‌ها را دچار خدشه کرده و در صورت عدم کنترل ممکن است سازمان‌ها را دچار زیان‌های مالی سنگینی بکند.

1- Wal-Mart

مسائل مربوط به حق انحصاری آثار و حریم خصوصی

سازمان‌های اینترنتی در برابر بحران‌های حقوقی خاص نیز آسیب‌پذیر هستند. ماجرای ناپستر برخی از مسائل مربوط به حق انحصاری آثار را نشان می‌دهد که اینترنت به آنها دامن می‌زند. ناپستر از طریق شبکه غیر متمرکز[1] برای مشتریان خود موسیقی مجانی ارائه می‌کرد. اما تهیه‌کنندگان موسیقی بر این باور بودند که این شرکت حق انحصاری آثار مربوط به آنها را نقض کرده و به این ترتیب منافع مالی آنها را به خطر می‌اندازد. تهیه‌کنندگان موسیقی بر علیه ناپستر اقامه دعوی کرده و نهایتاً این شرکت وادار گردید به ارائه خدمات مجانی پایان دهد. به دنبال این قضیه، فعالیت‌های ناپستر متوقف گردید، اما هنوز تعدادی از شبکه‌های غیر متمرکز وجود دارد که انواع مطالب را بطور غیر قانونی منتشر می‌کنند. در اگوست سال ۲۰۰٤، دولت فدرال در تلاش برای کاهش اینگونه فعالیت‌ها، برخی از این شبکه‌ها را برچید.(۷) رعایت حق انحصاری آثار برای مؤسسات آموزشی اینترنتی نیز الزامی شده است. در حال حاضر، آموزش اینترنتی به عنوان یک شیوه آموزش و منبع درآمد جدید برای برخی از دانشگاه‌ها محسوب می‌شود. به طور معمول، حق انحصاری مطالبی که اعضای هیئت علمی دانشگاه‌ها برای تدریس در کلاس‌های درس تهیه می‌کنند، مربوط به خود آنهاست. بنابراین آنها می‌توانند این مطالب را برای تدریس در دانشگاه‌های دیگر نیز مورد استفاده قرار دهند. موضوعی که در این ارتباط مطرح می‌باشد این است که حق انحصاری آثار در خصوص دوره‌هایی که دانشگاه‌ها از طری اینترنت ارائه می‌کنند، وضعیت خیلی روشنی ندارند.

همان طور که ماجرای شرکت ناپستر نشان می‌دهد، مسائل مربوط به حق انحصاری آثار ممکن است بقای یک سازمان را بطور جدی به مخاطره بیندازد. همچنین افشاگری‌های رسانه‌ایی باعث می‌شود سازمان‌ها برای اثبات مشروعیت و اعاده حیثیت خود به تلاش‌های زیادی دست بزنند. هزینه‌های مالی اینگونه تلاش‌ها

1- Peer-to-peer online medium

می‌تواند کارآیی سازمان‌ها را تضعیف کند.

اطلاعات خصوصی مشتریان نیز به یک دغدغه اصلی تبدیل شده است. مسائل حقوقی مربوط به شرکت‌هایی که اینگونه اطلاعات را در اختیار دیگران قرار می‌دهند در رسانه‌ها مورد تأکید قرار گرفته است. موضوع دیگری که رسانه‌ایی شده و به لحاظ حقوقی نیز دارای اهمیت می‌باشد این است که بعد از تعطیلی فعالیت‌های یک شرکت، تکلیف اطلاعات در اختیار آن چه می‌شود. هنگامی که شرکت تویزمارت[1] تعطیل گردید، پیشنهاد ۵۰ هزار دلاری شرکت دیزنی برای در اختیار گرفتن اطلاعات مربوط به مشتریان تویزمارت باعث جر و بحث‌های زیادی گردید (سندوال[2]، ۲۰۰۱). همچنین، دادستان‌های چندین ایالت بطور قطعی به این نتیجه رسیده بودند که اطلاعات مشتریان شرکت ایی‌تویز نمی‌تواند به دنبال ورشگستگی شرکت به طور مستقیم فروخته شود.

هنگامی که شرکتی آگاهانه و یا بطور ناخودآگاه با ارسال اطلاعات مشتریان به شرکت‌های دیگر، قوانین مربوط به حریم خصوصی را نقض می‌کند، بحران‌های روابط عمومی بروز می‌کند. این اتفاقات نیز پیامدهای مالی و حقوقی جدی را به دنبال دارند. برای مثال، در آوریل سال ۲۰۰۱، شرکت آلکس به عنوان یکی از شعب اینترنتی شرکت آمازن، مبلغ ۱/۹ میلیون دلار را برای پایان دادن به یک دعوای حقوقی پرداخت کرد. در این پرونده ادعا شده بود که آلکس با نقض قوانین مربوط به رعایت حریم خصوصی، اطلاعات محرمانه مشتریان را در اختیار آمازن قرار داده بود. این در حالی بود که شرکت آلکس در این پرونده به ارتکاب هیچ گونه خطایی اعتراف نکرد بود.(۸)

راهبردهایی برای مدیریت بحران

محققین مراحل مدیریت اثربخش بحران را به ترتیب زیر تقسیم‌بندی کرده‌اند:

1- Toysmart.com
2. Sandoval

۱. پیشگیری از بحران
۲. آمادگی برای بحران
۳. مهار بحران
٤. احیا
۵. عبرت‌آموزی از بحران (کوور- میزرا، زاموتو[1] و میترف، ۲۰۰۰؛ پیرسون و میترف، ۱۹۹۳)

به این ترتیب، سازمان‌ها حدالامکان باید از بحران‌ها جلوگیری کنند، اما در صورت بروز بحران آنها باید از آمادگی لازم برای مهار بحران، بهبود اوضاع و عبرت‌آموزی از آن برخوردار باشند. با این حال، بیشتر سازمان‌های اینترنتی هنوز در حال کسب توانمندی‌های لازم در حوزه مدیریت بحران هستند. همزمان با بروز اشکال جدید بحران، این سازمان‌ها گام‌های بلندی را در جهت کسب تجربه و اجتناب از آنها برداشته‌اند. بروز انواع مختلف بحران‌های اینترنتی نوعی آگاهی را در میان این سازمان‌ها بوجود آورده است و باعث پیدایش فرصت‌های جدید برای فراهم کنندگان زیرساخت‌ها و خدمات مربوطه گردیده است. برای مثال، به دنبال ناتوانی شرکت‌های اینترنتی برای پاسخگوئی به انبوه مراجعه کنندگان در سال ۱۹۹۹، اکنون برخی از شرکت‌ها مانند شرکت مرکوری اینتراکتیو[2] خدماتی را ارائه می‌کنند که می‌توان به وسیله آنها توانائی سایت‌های تجاری را با ترافیک مصنوعی ایجاد شده تست کرد. همچنین، تعدادی از شرکت‌های امنیتی پا به عرصه گذاشته‌اند که از یک سو محصولات و خدماتی را برای شناسایی آسیب‌پذیری‌ها از طریق ممیزی‌های امنیتی در اختیار شرکت‌های اینترنتی قرار می‌دهند و از سوی دیگر، نظارت و کنترل سیستم‌های آنها را به عهده می‌گیرند.

ادبیات مدیریت بحران انبوهی از راهبردها را عرضه کرده است که سازمان‌های اینترنتی می‌توانند از آنها بهره جویند (بارتون[3]، ۱۹۹۳؛ فینک، ۱۹۸٦؛ کوور- میزرا،

1. Zammuto
2. Mercury Interactive
3- Barton

۱۹۹۵؛ پاچنت و میترف، ۱۹۹۲؛ پیرسون و میترف، ۱۹۹۳). برای مثال، آماده‌سازی برنامه‌ها و تیم‌های مدیریت بحران، تشکیل اتاق کنترل، استفاده از ممیزی یادگیری، و مدیریت فشار روانی کارکنان راهبردهای ارزشمندی برای مدیریت بحران در سازمان‌های اینترنتی هستند.

ما در این نوشتار هفت راهبرد را معرفی می‌کنیم که به اعتقاد ما رهبران سازمان‌های اینترنتی می‌توانند برای مدیریت بحران‌ها بهترین استفاده را از آنها به عمل بیاورند. این راهبردها بر اساس مراحل مدیریت بحران در جدول (۲) معرفی شده‌اند.

جدول ۲: راهبردهای مدیریت بحران برای سازمان‌های اینترنتی با در نظر گرفتن مراحل مدیریت بحران

راهبرد پیشنهادی	مراحل مدیریت بحران				
	آمادگی	پیشگیری	مهار	احیا	عبرت‌آموزی
مسائل فنی و گروه-های گفتگو را کنترل کنید					
ذینفعان اصلی را شناسایی کنید					
در برابر بحران‌های اینترنتی آمادگی داشته باشید					
مراکز داده ثانوی ایجاد کنید					
به ابعاد غیر فنی بحران‌های اینترنتی بپردازید					
روابط با مشتری را مدیریت کنید					
از تجارب سازمان‌های اینترنتی در خصوص بحران استفاده کنید					

توجه: قسمت‌های رنگی نشان‌دهنده راهبرد یا راهبردهای مورد استفاده در مراحل مختلف می‌باشند.

کنترل مسائل فنی و گروه‌های گفتگو

مدیران ارشد باید از طریق کنترل سیگنال‌های فنی و سیگنال‌های مربوط به گروه‌های گفتگو، تهدیدهای ناشی از ذینفعان اصلی، به ویژه هکرها، را شناسایی کنند. تهدید وب سایت یکی از تهدیدات جدی بر علیه یک سازمان اینترنتی است. سازمان‌ها باید بتوانند حملات سرکاری را از حجم فزاینده مشتریان قانونی خود تفکیک کنند. همچنین لازم است آنها سیستم‌های امنیتی ضروری را در اختیار داشته باشند تا از حمله به مراکز اطلاعات مشتریان خود آگاه شوند. هم‌اکنون برای تهیه ابزارهای هشدار دهنده ورود غیر قانونی به سیستم‌ها، فعالیت‌هایی در حال انجام است، اما تا زمان استفاده عملی از اینگونه ابزارها فاصله زیادی وجود دارد. از طرفی، ماهیت پیوسته متغییر اینگونه حملات کار طراحی سیستم‌های امنیتی مطمئن را پیچیده‌تر کرده است. کی‌نوت[1] و مرکوری اینتراکتیو نمونه‌هایی از سازمان‌هایی هستند که از طریق کنترل بیرونی، یک سری هشدارهای اولیه را در خصوص مشکلات بالقوه مربوط به سایت‌ها می‌دهند.

گروه‌های گفتگو که مخاطبین را به یکدیگر متصل می‌کنند، در دسترس اعضای سازمان مرکزی هستند. برای تشخیص محور و لحن مباحث، می‌توان گروه‌های گفتگوی مربوط به سازمان را به طور پیوسته کنترل کرد. با کنترل اتاق‌های گفتگو و تابلوی اعلانات مجازی هکرها، کارشناسان امنیتی اغلب می‌توانند اطلاعات ارزشمندی در خصوص مقاصد آنها بدست بیاورند. تابلوهای بحثی که سایت‌های تجاری مانند یاهو، فاینانس و کویکن[2] نیز در اختیار مراجعه‌کنندگان قرار می‌دهند، می‌توانند اطلاعات مفیدی را فراهم کنند. سایت دیگری بنام تیم واکنش سریع کامپیوتری[3] نیز مجموعه‌ایی از آسیب‌پذیری‌ها و حملات شناخته شده را در اختیار دارد که لازم است کارشناسان فن‌آوری اطلاعات آنها را به طور مرتب کنترل کنند.

1- Keynote
2- Quicken
3- The Computer Emergency Response Team (CERT)،

شناسایی ذینفعان اصلی در محیط اینترنت

دومین راهبرد برای جلوگیری و کنترل بحران‌ها عبارت از شناسایی ذینفعانی است که در فضای اینترنتی دارای نقش مهمی هستند. در اینجا منظور از ذینفع فرد یا گروهی است که بر یک سازمان تأثیر گذار بوده و یا از آن تأثیر بپذیرد (فریمن، ۱۹۸٤). به غیر از ذینفعان متعارف یک سازمان مانند مشتریان، کارکنان، سرمایه‌گذاران، رقبا، تأمین‌کنندگان نیازها، و رسانه‌ها، ذینفعان دیگری مانند هکرها، ارائه‌کنندگان خدمات اینترنتی، کارشناسان مراکز داده، یا تیم واکنش سریع رایانه‌ایی نیز باید مورد توجه قرار گیرد.

می‌توان از ارزیابی ذینفعان برای شناخت نگرش آنها استفاده کرد – اینکه آیا آنها نسبت به سازمان نگرش خصمانه، دستگیرانه، دوستانه، یا بی‌طرفانه دارند. میزان تأثیرگذاری منفی آنها بر سازمان نیز باید مورد ارزیابی قرار گیرد (ساویج، نیکس، وایت‌هد و بلیر[1]، ۱۹۹۱). سازمان‌ها ممکن است به این نتیجه برسند که نگرش ذینفعان آنها هم خصمانه و هم دستگیرانه است و آنها از قدرت تأثیرگذاری بالایی بر سازمان برخوردار هستند. با بررسی این دو گروه معلوم می‌شود که ذینفعان اصلی کدام‌ها هستند و چه افراد یا گروه‌هایی دوست یا دشمن می‌باشند. برای مثال، در صورتی که سازمان در برگرداندن سود سرمایه‌گذاران کند عمل کند، آنها ممکن است نگرش خصمانه‌ایی نسبت به سازمان پیدا کنند. چنین سازمانی ممکن است خود را مورد هدف هکرهای خاصی ببیند. جنبه مثبت قضیه این است که کارکنان سازمان ممکن است نگرش وفادارانه و حمایتی داشته و رسانه‌های محلی ممکن است به دلایل تعصبی در پی معرفی کارکردهای مثبت سازمان باشند. لازم است برای خنثی کردن فعالیت‌های ذینفعان متخاصم و تقویت روابط با ذینفعان همدست تلاش کافی صورت پذیرد. ارزیابی‌های قبل از بحران در خصوص ذینفعان می‌تواند شرایط بالقوه بحرانی را روشن کرده و برای خنثی کردن

1- Savage, Nix, Whitehead, and Blair

آن کمک کند. در طول یک بحران، نتایج ارزیابی‌ها می‌تواند به سازمان کمک کند تا راهبردهای مدیریت بحران را برنامه‌ریزی کند.

کسب آمادگی در برابر بحران‌های اینترنتی

محققان مدیریت بحران اهمیت کسب آمادگی در برابر بحران‌ها را خاطر نشان کرده‌اند. گفته می‌شود سازمان‌هایی که خود را برای بحران خاصی آماده کنند، می‌توانند از این آمادگی در ارتباط با بحران‌های مشابه نیز استفاده کنند (پیرسون و میترف، ۱۹۹۳).در این مقاله انواع بحران‌های فراروی سازمان‌های اینترنتی تشریح گردید. بنابراین، پیشنهاد می‌شود سازمان‌ها خودشان را برای مشکلاتی از قبیل خرابی (فنی) وب سایت، خرابکاری و باج‌خواهی (انسانی و اجتماعی)، تحریم‌های اینترنتی (روابط عمومی)، و مسائل (حقوقی) مربوط به حق انحصاری آثار و حریم خصوصی آماده کنند.

رشد و تحول پیوسته از دیگر ویژگی‌های مخاطرات مربوط به دنیای مجازی می‌باشد. به دنبال واکنش میکروسافت در برابر حملات سرکاری به سرورهای دی ان اس خود از طریق توزیع سرورهای دی ان اس در تمام شبکه توزیع آکامای[1]، هکرها حمله مشابهی را به شبکه آکامای صورت دادند. بنابراین، تلاش برای حرکت یک گام جلوتر و پیش‌بینی ماهیت حملات بالقوه کار بسیار سختی است. برخی شرکت‌های امنیتی خدماتی را بنام «هکر اخلاقی» آغاز کرده‌اند و تلاش می‌کنند همانند هکرهای واقعی به شبکه و کامپیوترهای یک شرکت حمله کنند. این کار اغلب باعث می‌شود آسیب‌پذیری‌های بالقوه و انواع جدید حملات ممکن شناسایی شود. همچنین شرکت‌های امنیتی خدماتی را با هدف شناسایی ورود غیر قانونی به سیستم‌ها ارائه می‌کنند که ضمن شناسایی اینگونه مزاحمت‌ها، به طور

۱- شرکت تولیدکننده نرم‌افزار برای ارائه محتوا در اینترنت

اتوماتیک اطلاعات مربوط به آخرین موارد از این نوع مزاحمت‌ها از طرف هکرها را در اختیار مسئولین مربوطه قرار می‌دهند. لازم است توجه داشته باشیم که ماهیت و شکل بحران‌های اینترنتی به سرعت در حال تغییر است و از این رو برای مواجهه با انواع جدید بحران‌های اینترنتی، لازم است سازمان‌ها آمادگی‌های خود را در برابر بحران‌ها روزآمد بکنند.

ایجاد مراکز داده ثانوی

از آنجایی که وب سایت سازمان‌های اینترنتی نقش بسزایی در کسب درآمد دارند، لازم است آنها در طراحی وب سایت‌ها، سیستم‌های جایگزین را در نظر بگیرند. با این کار آنها خواهند توانست در صورت مورد حمله قرار گرفتن اوضاع را به حالت عادی برگردانند. درست است که طراحی سیستم‌های جایگزین کارآمد کار پر هزینه‌ایی است، ولی هدف تیم‌های فنی باید این باشد که اِشکالات و ضعف‌های سیستم را به صفر برسانند. حتی در صورتی که سازمان از توانایی مالی لازم برای طراحی و استفاده از مرکز داده ثانوی را نداشته باشد، لازم است از آمادگی لازم در برابر بحران برخوردار باشد تا بتواند در صورت پیدا شدن مشکل جدی در مرکز داده اصلی، از امکانات جانبی برای فعال کردن سایت استفاده کند. همچنین شرکت‌ها باید از پوشش بیمه‌ایی کافی برخوردار باشند تا بتوانند در صورت بروز مشکلات به فعالیت خود ادامه دهند. برخورداری از این گونه آمادگی‌ها به سازمان‌ها کمک می‌کند تا خسارات را به حداقل رسانده و به سرعت اوضاع بحرانی را به حالت عادی برگردانند.

توجه به ابعاد غیر فنی بحران‌های اینترنتی

سازمان‌های اینترنتی کارشناسان فن‌آوری زبده‌ایی دارند و مسائل مربوط به فن‌آوری را جدی‌تر دنبال می‌کنند. بنابراین، ممکن است آنها ابعاد فنی بحران را

بیشتر مورد توجه قرار داده و برخی از ابعاد غیر فنی مانند نقش منفی رسانه‌ها، روابط بین مشتریان، یا خستگی روانی کارکنان خود را نادیده بگیرند. واکنش شرکت اینتل در برابر مشکل فنی مربوط به پردازش‌گر پنتیوم نمونه‌ایی از این نوع برخوردها می‌باشد. وقتی که مشکل فوق رسانه‌ایی گردید، شرکت اینتل شروع به بحث در مورد مسائل فنی از قبیل تأثیر محدود این مشکل در عملیات‌های روزمره کرد. آنها از تشخیص و پرداختن به ابعاد روابط عمومی این مشکل غافل بودند. این مسئله عکس‌العمل‌هایی را موجب شد و اینتل نهایتاً مجبور شد بعد از تحمل زیان مال و خدشه‌دار شدن حیثیت خود، پردازش‌گر فوق را جمع‌آوری کند.

سازمان‌های اینترنتی باید بدانند که ابعاد غیر فنی بحران نیز از اهمیت قابل توجهی برخوردار است. برای مثال، به دنبال یک حمله سرکاری، مسئولین امر علاوه بر توجه به ابعاد فنی مربوط به فعال کردن دوباره سایت، باید به ترمیم روابط خود با مشتریان نیز بپردازند. همچنین آنها باید نظرات شرکت را در رسانه‌ها منعکس کنند و بعد از سپری شدن بحران، به مشکلات روحی کارکنان نیز بپردازند. بنابراین، استفاده از افراد کارامد برای مدیریت ابعاد غیر فنی بحران از اهمیت زیادی برخوردار است.

مدیریت روابط با مشتری

توجه به مدیریت روابط با مشتری از آن جهت اهمیت دارد که اعتبار و حیثیت سازمان‌های اینترنتی مرهون مدیریت خوب این نوع روابط است. بنابراین، از دست رفتن اعتماد مشتریان بخاطر داشتن یک وب سایت نامطمئن یا عدم توانایی تحویل و ارائه کالاها و خدمات می‌تواند به شدت امکان داشتن روابط بلند مدت با آنها را تحت تأثیر قرار داده و مانع برگشت سازمان از وضعیت بحران به شرایط عادی گردد.

فروشندگان اینترنتی باید به سه اصل کسب اعتماد مشتری – وب سایت سریع و پایدار، پاسخگویی سریع و مطمئن به سفارشات، و خدمات عالی به مشتریان – بیشترین اهمیت را قائل شوند. لازم است مدیریت روابط با مشتری به طور ویژه مورد توجه قرار گیرد تا سازمان‌ها بتوانند مشتریان خود را شناخته و نیازهای آنها را به شکل مؤثر تأمین کنند. برای نشان دادن اهمیت این روابط باید تلاش زیادی صورت گیرد. برای مثال، به دنبال ناتوانی شرکت تویزروس در تحویل بهنگام سفارشات در ایام کریسمس سال ۱۹۹۹، برای ترمیم این ضایعه، شرکت فوق تلاش کرد تا هدایای صد دلاری به مشتریان خود ارسال کند.(۹) در آخر، باید گفت شواهد حکایت از آن دارند که عبرت‌آموزی از بحران‌ها و ایجاد تغییرات در جلب اعتماد مجدد ذینفعان نقش مؤثری دارد.

استفاده از تجارب سازمان‌های اینترنتی در خصوص بحران

از بحران‌ها می‌توان درس‌های زیادی آموخت، زیرا آنها ضعف‌ها و قوت‌های سازمان‌ها را نشان داده و پنداشت‌های موجود را به چالش می‌کشند. سازمان‌ها می‌توانند به طور مستقیم یا غیر مستقیم از تجارب دیگران درس بگیرند (کوور- میزرا، ۱۹۹٦). محققین می‌گویند برای کسب تجربه مؤثر از بحران‌ها، مدیران ارشد فضای مثبتی را برای عبرت‌آموزی از بحران بوجود می‌آورند، از تیم‌های آموزشی چند منظوره استفاده می‌کنند، رفتارهای یادگیری را تشویق می‌کنند، و تغییرات ضروری را دنبال می‌کنند (کوور- میزرا و ناتان[1]، ۲۰۰۰). به اعتقاد ما همه این راهبردها برای سازمان‌های اینترنتی کاربرد دارند. اما پیشنهاد ما این است که از تجربیات همه سازمان‌های اینترنتی استفاده شود. در حال حاضر، ما شاهد استفاده از تجربیات دیگران در صنایع با تجربه‌ایی مانند صنایع شیمیایی و صنایع هوایی هستیم. با توجه به این واقعیت که بروز بحران در بخشی از یک صنعت همه آن را

1- Nathan

تحت تأثیر قرار می‌دهد، هنگامی که سازمانی دچار بحرانی مانند نشت گاز یا سقوط هواپیما می‌شود، برای دیگر اعضای صنعت مربوطه فرصت داده می‌شود تا از حوادث پیش آمده کسب تجربه کنند. بحران‌هایی مانند حملات سرکاری، تحریم‌های اینترنتی، باج‌گیری، و خرابکاری می‌توانند موجب سلب اعتماد از همه سازمان‌های اینترنتی شوند. بنابراین، پیشنهاد می‌شود برای توانمندسازی کل صنعت مربوطه، سازمان‌ها علاوه بر کسب تجربه از اتفاقات مربوط به خود، از اطلاعات مربوط به دیگران نیز استفاده کنند.

جهت‌گیری‌های آینده در تحقیقات مدیریت بحران

بروز بحران‌های اینترنتی برای تحقیقات دانشگاهی در حوزه مدیریت بحران نیز مضامینی در بر دارد. اولاً، لازم است ابعاد دیگری به مدل‌های موجود گونه‌شناسی‌های بحران اضافه شود. مدل‌های فعلی، بحران‌ها را بر اساس متغیرهایی مانند شدت بحران، ریشه و علت اصلی بحران، یا حوزه تأثیر بحران تقسیم‌بندی می‌کنند. گونه‌های اینترنتی بحران ابعاد دیگری مانند محدوده جغرافیایی و سرعت تشدید را مطرح می‌کنند که لازم است در طرح‌های تقسیم‌بندی بحران در نظر گرفته شود.

اشکال اینترنتی بحران به مرزهای ملی محدود نمی‌شوند. بحران‌هایی مانند آتش‌سوزی و انفجار ممکن است یک منطقه جغرافیایی خاصی را در بر گیرند، اما بحران‌های اینترنتی از قبیل تحریم‌ها و خرابکاری‌های مجازی کل جهان را در بر می‌گیرند، و ذینفعان آنها ممکن است در کشورهای دیگری حضور داشته باشند. در برخی از نمونه‌هایی که مورد بحث قرار گرفت، هکرها در چین، فیلیپین، و کانادا مستقر بودند. محدوده جغرافیایی بحران متغیر مهمی است که بخاطر تأثیر آن بر چهارچوب برنامه‌ریزی و اقدامات مربوط به مدیریت بحران باید مورد توجه قرار گیرد.

سرعت تشدید بحران مؤلفه دیگری است که لازم است بـه گونـه‌شناسـی‌هـای بحران اضافه گردد. بحران‌ها سرعت تشدید متفاوتی دارند. برای مثال، بحـران‌هـایی مانند تحریم‌های مجازی نسبت به اشکال دیگر تحـریم از سـرعت تشـدید بـالایی برخوردارند، زیرا اینترنت اطلاعات را بسرعت در اختیار همگان قرار می‌دهـد. هـر چقدر سرعت تشدید بحران بالاتر باشد، به همـان میـزان ضـرورت کنتـرل بحـران افزایش پیدا می‌کند. بنابراین، لازم است مدل‌های تقسیم‌بندی بحران ایـن متغییـر را در تقسیم‌بندی بحران‌ها در نظر بگیرند.

دوماً، در معرض تهدید بودن سازمان‌ها و مشهود بـودن بحـران‌هـا بـرای مـردم مؤلفه‌های دیگری هستند که لازم است در ارزیابی آسیب‌زایی بحران‌ها مورد توجـه قرار گیرند. این عوامل، سازمان‌های اینترنتی را در برابر بحران‌ها مستعدتر می‌کننـد. مدل‌های بررسی علل بحران بطور معمول عوامل سازمانی مانند سـاختار، فرهنـگ، فن‌آوری و فقدان عناصری مثل برنامه و روش را مورد توجه قرار داده‌اند. اینترنـت سازمان‌ها را بیشتر در معرض مخاطرات قرار می‌دهد. وب سـایت‌هـا و مراکـز داده سازمان‌ها می‌توانند هر ساعت از روز یا شب و از هر نقطه جهان مورد هدف افـراد مغرض قرار گیرند. بعلاوه، وقتی که فعالیت وب سایتی متوقف می‌شود و یا حملـه سرکاری به آن صورت می‌گیرد، ناظران مستقر در هر نقطه‌ایی از دنیا این مسـائل را مشاهده کرده و از مشکلات سازمان آگاهی پیدا می‌کنند. در معـرض تهدیـد بـودن سازمان‌ها و مشهود بودن بحران‌ها برای دیگران مؤلفه‌هایی هستند کـه بایـد هنگـام ارزیابی آسیب‌پذیری سازمان در مقابل بحران‌ها مورد توجه قرار گیرند.

و بالاخره، سازمان‌های سنتی که وارد عرصه مجازی می‌شوند، نمونه‌های جالبی برای مطالعه چگونگی سازگاری مدیران با تغییرات در محیط‌های بحران و آمـادگی آنها در برابر بحران می‌باشند. به طور معمول، سـازمان‌هـای مجـازی در مقایسـه بـا سازمان‌های سنتی فرهنگ‌های متفاوت‌تری دارند، زیرا محیط آنها متفـاوت اسـت و

آنها با ذینفعان متفاوت چه به عنوان کارکنان خود و چه به عنوان هکر سروکار دارند. ارزش‌ها و زبان آنها نیز متفاوت است. توانایی مدیران برای عبور از فرهنگ سنتی خودشان، پذیرش گونه‌های جدید بحران از طرف آنها، و کسب آمادگی بیشتر برای بحران‌ها مسائلی هستند که می‌توانند به ما کمک کنند تا از چگونگی واکنش مدیران در برابر مخاطرات بالقوه و از نحوه آمادگی آنها در برابر بحران شناخت عمیق‌تری پیدا کنیم.

به عنوان نتیجه‌گیری، باید خاطر نشان کرد که اینترنت به عنوان ابزاری برای انجام فعالیت‌های تجاری در آینده نیز در خدمت بشریت خواهد بود. هم‌زمان با افزایش وابستگی‌های ما به این رسانه، لازم است نسبت به مخاطرات ذاتی آن و انواع بحران‌های ناشی از آن شناخت بهتری پیدا کنیم. در اینجا، تلاش کردیم مسائل فوق را روشن کرده و برای مدیریت بهتر آنها راهبردهایی را برای مدیران ارشد معرفی کنیم، و به منظور پرداختن به پیچیدگی‌های بحران‌های «دنیای مجازی» دامنه تحقیقات آکادمیک را گسترش دهیم.

پی‌نوشت‌ها

1- MafiaBoy pleads guilty in hacker case, http://news.cnet.com/news/0-1005 - 200-45 23 2 77 .html.
2- Global hacker agreement could affect bug hunters, http://news.cnet. com/news/0-1005-200-3314003.html.
3- Outages plague eBay again, http://news.cnet.com/news/0-1007-200-344247.html.
4- See www.toywar.com and eToys settles net name dispute with etoy, http://news.cnet.com/news/0-l007 -200-1531854.html.
5- See Toysrus.com's net congestion continues, http://news.cnet.com/news/0-1006-200-1435578.html.
6- See FBI probes extortion case at CD store, http://news.cnet.com/news/ 0-] 007 - 200-15] 9088.html; Borland, op. cit.
7- http://www.cnn.com/2004/TECH/08/26/cybercrime.probe.
8- Amazon unit settles privacy lawsuit, http://news.cnet.com/news/ 0-1007 -200-5754965.html.
9- See Toys "R" Us falling short on Christmas deliveries, http://ne\\'s.cnet.com/ news/0-1007 -200-150310 l.html.

منابع

Akamai says Internet attack disrupted major Web sites. (June 15, 2004). Associated Press.

Barton, L. (1993). *Crisis in organizations: Managing and communicating in the heat of chaos.* Cincinnati, OH: South-Western Publishing.

Borland, J. (2000, March 2). Hacker attack latest in string of online credit card thefts. Retrieved December 29, 2006, from http://news.com.com/2100-1017-237553.html

Fink, S. L. (1986). *Crisis management: Planning for the inevitable.* New York: AMACOM.

Freeman, R. E. (1984). *Strategic management: A stakeholder approach.* Englewood Cliffs, NJ: Prentice Hall.

Hambrick, D. c., &D' Aveni, R. A. (1988).Large corporate failures as downward spirals.*Administrative Science Quarterly,* 33, 1-23.

Kovoor-Misra, S. (1995). A multi-dimensional approach to crisis preparation for technical organizations: Some critical factors. *Technological Forecasting and Social Change,* 48, 143-160.

Kovoor-Misra, S. (1996).Moving towards crisis preparedness: Factors that motivate organizations.*Technological Forecasting and Social Change,* 53, 69-183.

Kovoor-Misra, S., Clair, J. A., &Bettenhausen, K. L. (2001).Clarifying the attributes of organizational crises.*Technological Forecasting and Social Change, 67,* 77-91.

Kovoor-Misra, S., &Nathan, M. (1999). Crisis causation re-framed. *Central Business Review,* 18(2),29-35.

Kovoor-Misra, S., &Nathan, M. L. (2000). Timing is everything: The optimal time to learn from crises. *Review of Business,* 21(3),3]-36.

Kovoor-Misra, S., Zammuto, R. E, &Mitroff, I. I. (2000). Crisis preparation in organizations: Prescription versus reality. *Technological Forecasting and Social Change,* 63, 43-62.

Lemos, R., &Charny, B. (2000, December 22). Hackers crack Egghead.com.

Retrieved December 29, 2006, from http://news.com.com/2009-1017-250262.ht1111

Musil, S. (2000, September 10). Western Union Web site hacked. Retrieved December 29,2006, from http://news.com.com/2100-1023-245525.html

Nystrom, P. c., &Starbuck, VV. H. (1984). To avoid organizational crises, unlearn. *Organizational Dynamics,* 12(4),53-65.

Pauhant, T. c., &Mitroff, I. I. (1992).*Transforming the crisis-prone organization.*San Francisco: Iossey-Bass.

Pearson, C. M., &Clair, J. A. (1998). Crisis management re-framed. *Academy of Management Review,* 23, 59-78.

Pearson, C. M., &Mitroff, I. I. (1993). From crisis prone to crisis prepared: A framework for crisis management. *The Academy of Management Executive,* 7(1),48-59.

Sandoval, (~. (2001, January 31). Judge OKs destruction of Toysmart list. CNET News.Com. Retrieved December 29, 2006, from *http://news.com.com/2104*-1017 _3-251893.html

Savage, G. I., Nix, l'. W., Whitehead, C. J., &Blair, J.D. (1991).Strategies for assessing and managing organizational stakeholders.*Academy of Management Executive,* 5(2),61-75.

Achmeltzer, J. (2004, May 20). Caribou grinds away at rumor. Chicago Tribune.com. Retrieved December 29, 2006, from http://www.kellogg .northwestern.edu/news/hits/040520ct.htm

Shrivastava, P. (1987). *Bhopal: Anatomy of a crisis.* Cambridge, MA: Ballinger.

Turner, B. A. (1976). The organizational and inter-organizational development of disasters.*Administrative Science Quarterly,* 21, 378-397.