عصر تجارت الکترونیک و لزوم خرید پوشش های بیمه ای در مقابل خطرات جدید ناشی از حضور مجرمان اینترنتی

مجرمان اینترنتی می توانند صدمات شدیدی به رایانه های شرکت ها و حتی اشخاص بدون بر جای گذاشتن کوچکترین ردپائی (نه اثر انگشتی، نه آثار شلیک گلوله ای و نه حتی ته سیگاری) وارد نمایند.

اینترنت این توانائی را دارد که به رهبران گروهها، مجریان و مدیران ارشد مؤسسات مالی، قانونگذاران، مامورین امنیتی در سطح بالا، مدیران ریسک و دلالان یا واسطه های بیمه کمک نماید یا اینکه ضرر و زیان برساند.

اینترنت یا سایر پروتکل های انتقال داده ها، سبب تسهیل در جریان و پردازش اطلاعات شده اند. دراقتصاد جدید، اطلاعات، سرمایه اولیه و مایع حیاتی (همانند خون در شریان ها) در هر شرکتی است و شرکت ها محتاطانه از آن محافظت می کنند. حتی شرکت هائی که به خوبی اداره و کنترل می شوند نیز به مباحثه و گفتگو درباره امنیت اطلاعات و مسائلی چون فن آوری اطلاعات (Information Technology) که به راه حل های اطلاعاتی نیاز دارد، علاقه نشان می دهند.

پوشش کامل شرکت

اطمینان از امنیت اطلاعاتی و ساختار اطلاعاتی سازمان موضوعی است که در سطح کل شرکت مطرح است و مسئولیت آن بر عهده مدیران عالی رتبه (اعضای هیئت مدیره) و سایر اشخاص مهم در سازمان است.

هرگونه اشکالی در امنیت شبکه اطلاعاتی سازمان اثرات گسترده و مخربی در سراسر سازمان دارد. در کل، نقص در خدمت رسانی یا قطع آن می تواند تا حدود زیادی بر سطح عملیاتی سازمان اثر بگذارد به گونه ای که یقیناً در چنین حالتی اگر اخبار و اطلاعات دچار نقص و اختلال گردند نام تجاری و شهرت سازمان آسیب خواهد دید.

جورج دبلیو تنت (George W. Tenet) مدیرشبکه سی آی ای (CIA) می گوید: "ادامه حیات ما در گرو استفاده از اطلاعات است و به منظور افزایش اطلاعات بیش از پیش به شبکه های رایانه ای وابسته می شویم و اکنون نیز برای پذیرش مشتریان از شبکه اطلاعاتی استفاده می کنیم. قابلیت اعتماد،

سبب وابستگی می شود و وابستگی نیز آسیب پذیری را به دنبال دارد."

عوامل داخلی

ضربه پذیری در اکثر موارد علت داخلی دارد. زمانی که از کلاهبرداری و تقلب در اقتصاد جدید صحبت می شود رسانه های چاپی یا الکترونیکی همه تقصیرها را متوجه هکرها می دانند. اما جورج دبلیو تنت معتقد است که ریشه اصلی خطرات در داخل سازمان ها است .

دست اندرکاران داخلی شامل کارمندان، مشتریان و شرکای قدیمی، همگی کسانی هستند که اجازه دسترسی به شبکه های رایانه ای شرکت را دارند و با قواعد دیوارهای آتش (Firewall)[۱] آشنائی دارند لذا تهدید بیشتری را موجب می شوند. برای مثال ؛ اشخاصی که به سیستم های اطلاعاتی شرکت ها دسترسی دارند، می توانند به اطلاعات مشتریان آسیب رسانده و داده های مشتریان، اطلاعات قیمت گذاری، اطلاعات مربوط به محصولات جدید، اطلاعات مالی، امضاهای الکترونیکی و یا کدهای مخصوص مدیران را به سرقت ببرند، در حالی که وابستگی شرکت ها به این اطلاعات هر روز بیشتر می شود و اغلب شرکت ها به صورت انباری از اطلاعات محرمانه مشتریان و مالکان در می آیند.

اختلال در امنیت شبکه

مسئله مهم این است که ارزش اطلاعات در تجارت درسال های اخیر رشد بی نظیری داشته است. زیرا شرکت ها به تدریج از فرایندهای سنتی تجاری تغییر مسیر داده و به دارائی های هوشمند متکی به فن آوری وب روی آورده اند.

اختلال در امنیت شبکه ها ممکن است برای مدت طولانی کشف نشده باقی بماند و سبب خسارات قابل توجهی شود همچنین شرکت ها نیز به تاخیر در گزارش دهی اختلالات ناشی از عدم صداقت کارکنان، حملات اینترنتی (هک) و شکست های امنیت شبکه تمایل دارند که حل مشکل را به تاخیر می اندازد.

تهدیدات خارجی

علاوه بر تهدیدات داخلی که درستی و صحت شبکه اطلاعاتی شرکت را تحت تاثیر قرار می دهند تهدیدات بیرونی نیز وجود دارند که شرکت ها باید آن ها را جدی بگیرند یکی از این تهدیدات اساسی، به سرقت بردن اطلاعات با ارزش شرکت است.

اختلال در سرویس دهی الکترونیکی و به هم ریختن عملیات کاری شرکت و قطع ارتباط با مشتریان، عرضه کنندگان و شرکای تجاری نیز تهدیدات دیگری هستند که در شبکه وجود دارند و حتی وانمود کردن به حمله نیز امکان پذیر است. یک تهدید دیگر این است که با وارد آوردن ضربه از طریق شبکه شرکت را به منابع مالی نیازمند ساخته و سپس شرکت را خریده و در اختیار می گیرند. ویروس ها، کرم ها و انواع دیگر مخرب ها کماکان از خطرات اصلی در شبکه هستند. در حال حاضر مازاد بر ۵۶۰۰۰ نوع ویروس در شبکه وجود دارد و هر هفته ۵۰ نوع جدید به آن اضافه می گردد. دو چیز سبب حادتر شدن مشکل می شود: اول اینکه، ویروس هائی که ضمیمه (Attached)

فایل ها هستند و به کامپیوترها وارد می شوند، دوم اینکه، این ویروس ها به سرعت تکثیر شده و پراکنده می شوند.

جاسوسی، دشمنی با علم و صنعت و ناهنجاریهای اجتماعی (Vandalism and sabotage) خطرات معمول دیگری هستند که در امنیت شبکه ها وجود دارند. هیئت مدیره و مدیران عالی رتبه شرکت ها باید این خطرات و احتمال وقوع آنها را در اختلال شبکه درک کرده و در تصمیم گیری ها در نظر بگیرند.

جرائم واقعی و جرائم اینترنتی

جرائم اینترنتی همان تهدیدات و جرم های سنتی هستند با قدرت تخریب بیشتر و وسیع تر. (جدول ۱)

خطرات گوناگون.

درک ماتریس جرائم اینترنتی به تنهائی کافی نیست، بلکه شرکت ها باید در مورد اینکه اینترنت چگونه میزان و نوع خطرات را تغییر می دهد و چگونه باید این خطرات را پوشش داد، توجه جدی مبذول دارند. مسئله این است که اغلب پوشش های بیمه مسئولیت شرکت ها قدیمی بوده و ریسک های جدید که در اثر اینترنت ایجاد شده است، تحت پوشش بیمه ها قرار ندارند.

جدول ۱. جرائم در دنیای واقعی و در اینترنت

جرم	در دنیای واقعی	در اینترنت
دسترسی بدون اجازه	شکستن قفل ها و واردشدن	شکستن کلمه عبور یا رمز ورود
دشمنی با علم و صنعت	خرابکاری، آتش سوزی عمدی	ارسال ویروس و کرم ها به وب سایت
تولید مانع (کارشکنی)	ایجاد مانع فیزیکی	حمله به سیستم های عامل
سرقت (پول)	سرقت پول نقد	انتقال وجوه به صورت الکترونیکی (کارت های اعتباری)
سرقت (دارائیها)	سرقت دارائی مادی و فیزیکی	سرقت آدرس انتقال فایل ها در اینترنت، نرم افزارها و برنامه های کاربردی
جعل هویت	امضای جعلی	سرقت کدهای اطلاعاتی و شکستن قفل پست الکترونیک
سوء استفاده از دارائیهای شرکت	تجاوز به فضای پستی و امکانات شرکت	تخریب صفحات وب

برای نمونه، شرکت چاب (Chubb) در سال ۱۹۰۷ بیمه صداقت و امانت را معرفی نمود. اما این نوع بیمه تفییراتی اساسی داشته است و شرکت ها دریافته اند که بیمه صداقت و امانت امروزه نه تنها نیازشان را برآورده نمی سازد، بلکه خطرات جدیدی را که با آن مواجه هستند نیز پوشش نمی دهد.

منظور از امنیت اطلاعات در شبکه رایانه ای شرکت ها، کاهش تهدیدات اینترنتی به پائین ترین سطح ممکن است و برای این منظور شرکت ها باید بدانند چه خطراتی آنها را تهدید می کند و چگونه بایستی با انتقال این خطرات در عملیات کاری خود تعادل ایجاد کنند، در این حالت نقش شرکت های بیمه بسیار تعیین کننده است.

سه سطح پوشش نمونه

امروزه شرکت ها نیاز به سه نوع پوشش بیمه ای یا معادل آنها را دارند تا از خطرات بازرگانی، شغلی و خسارات بالقوه مربوط به اینترنت بکاهند. این پوشش ها عبارتند از:

۱- پوشش مسئولیت عمومی بازرگانی سی جی ال (CGL) که به آن چتر مسئولیت نیز می گویند.

۲- پوشش غرامت حرفه ای و اشتباهات و قصورات.

۳- جرائم مربوط به صداقت و امانت و جرائم الکترونیکی.

متاسفانه اکثر شرکت ها تنها پوشش نوع اول و پوشش مسئولیت مازاد را در برنامه هایشان دارند. این حالت آسیب جدی را در راهکارهای انتقال خطر سنتی وارد می کند. به خاطر داشته باشید که این راهکارها برای جلوگیری از خطرات در دنیای واقعی در نظر گرفته شده اند. در دنیای مجازی اینترنت، یک شرکت یا شخص می تواند بدون وارد شدن هیچگونه خسارت فیزیکی، متحمل زیان های بزرگی شود. برای مثال اختلال در امنیت و یا حتی تهدید به اختلال در امنیت شبکه رایانه ای شرکت مانند "سرک کشیدن به اطلاعات" سبب می شود مشتریان کارهایشان را به شرکت هائی که دارای امنیت بیشتری هستند، بسپارند و شرکت متحمل زیان شود. اما این خسارت از نوع فیزیکی نیست که بیمه های اموال یا بیمه های صداقت و امانت آنها را تحت پوشش قرار دهد. تصور کنید که سیستم مخابراتی یک شرکت به گونه ای باشد که کارمندان به دفاتر و بایگانی مدارک محرمانه مشتریان دسترسی داشته باشند. این خود نوعی آسیب پذیری است زیرا افشای بدون اجازه این مطالب خطایی است که باید بهای سنگینی بابت آن پرداخت. اما در رابطه با خساراتی که ناشی از عوامل زیر باشد چه باید کرد؟ عواملی چون :

ویروس ها، کرم ها، اشتباه در پرداخت صورت حساب ها، به سرقت رفتن اطلاعات کارت اعتباری و سوء استفاده ها و دیگر مواردی که در تجارت الکترونیکی روی می دهند.

چگونه شرکت ها خود را محافظت نمایند؟

با توجه به روش های سنتی انتقال ریسک یعنی: بیمه صداقت و امانت و بیمه های اشیاء و اموال وضعیت چگونه است. بیمه صداقت و امانت بعضی

خطرات را در تجارت الکترونیک تحت پوشش قرار نمی دهد، از جمله:

- خسارات حاصله از اطلاعات اختصاصی و محرمانه، خساراتی که به علت وقفه تجاری به وجود آمده باشد و یا وام هائی که از طریق شبکه رایانه ای پرداخت شده اند.
- بیمه نامه جرائم اینترنتی بعضی ازخسارات را پوشش نمی دهد، مانند خسارت ناشی از سیستم های غیرمحرمانه (شبکه های غیر شخصی و گروهی)، خسارات ناشی از استفاده کنندگان مجاز که از میزان دسترسی خود فراتر رفته اند، زیان های حاصل از مطالب و اطلاعات محرمانه (اسرار تجاری)، انتقال ویروس از دستگاهی به دستگاه دیگر و اختلالات شغلی یا هزینه هائی که به حفظ عملکردها و بهره برداری یک شرکت تجاری در اوضاع بحرانی ضرر می رساند. بیمه اموال، خسارات مربوط به پول نقد و اوراق بهادار تجاری را که بانک ها و مؤسسات مالی، اختلاس در مدارک و دفاتر بایگانی، اختلالات کاری و هزینه هائی را که به واسطه آن به وجود می آیند تحت پوشش قرار نمی دهد.

خطرات مسئولیت مدنی شخص ثالث

ذکر این نکته مهم است که در بیشتر موارد هنگام تمدید قرارداد بیمه اتکایی، بیمه گران اتکایی بزرگ پوشش خساراتی را که به واسطه ویروس ها و مخرب های دیگر به وجود می آیند، محدود نموده و یا اصلاً قبول نمی کنند. جدای از این استثنائات که شرکت ها را در معرض خطر قرار می دهد، خطرات مسئولیت مدنی شخص ثالث نیز در جهان پهناور تجارت الکترونیک وجود دارد که اغلب توسط بیمه نامه های استاندارد سی جی ال تحت پوشش قرار نمی گیرند. این خطرات هنگامی دارای اهمیت خواهند بود که در زمره جرائم اینترنت قرار گرفته باشند، شرکت ها مجبور به محافظت خود در مقابل این خطرات اضافی هستند.

این خطرات چه مواردی می باشند؟ برخی از عمده ترین موارد عبارتند از :

۱- تجاوز به مطالب محرمانه: تجارت الکترونیک تهاجم به شرکت ها، تخلف یا مداخله در مطالب محرمانه را امکان پذیر می سازد و این موارد می تواند در مکان هایی که اطلاعات جمع آوری و منتشر می گردد و به اطلاع عموم می رسد، صورت گیرد و برای اشخاص ثالث ایجاد خسارت نماید.

۲- تجاوز به حقوق و دارائی های معنوی: در این مورد نیز یک شرکت که به تجارت الکترونیک می پردازد می تواند در صورت تجاوز به حقوق و دارائی های معنوی مجرم شناخته شود. این موارد شامل: تصاحب حق اختراع، علائم تجاری، حق چاپ و حفاظت از طرح ها و نظایر آن است.

۳- خسارت وارده به اطلاعات رایانه ای شخص ثالث، نرم افزار، برنامه ها و شبکه های رایانه ای: ارتباط متقابل با عرضه کنندگان و پیمانکاران شبکه های رایانه ای ممکن است به آسانی برای شرکت ایجاد مسئولیت نماید، به عنوان مثال شرکت سبب انتقال ویروسی به شبکه شرکت های دیگر گردد. برای مقابله با برخی از این خطرات صنعت

بیمه راه حل هائی را ارائه داده است. برای مثال شرکت چاپ امنیت در مقابل جرائم اینترنتی را توسط "بیمه جرائم اینترنتی برای مؤسسات مالی"، بیمه نموده است. این بیمه نامه آسیب پذیری مالی را در یک بیمه نامه پوشش می دهد. شرکت چاپ همچنین "بیمه مسئولیت مدنی شبکه اینترنت" را برای پوشش خطرهای مسئولیت مدنی بازرگانی (مربوط به تجارت الکترونیک) معرفی کرده است و در حالی که، بیمه نامه های جدید به میزان زیادی به شرکت ها در فائق آمدن در برابر خطرات کمک می نمایند، بهترین روش برای کاهش خطرهای تجارت الکترونیک تشویق مدیران و کارکنان سازمان به درک درست خسارت ها و پیامدهای ناشی از اختلال در امنیت شبکه است.

گامهائی که باید برداشته شوند

شرکت ها باید با استفاده از معیارهای زیر اقدام کنند:

۱- دسترسی و مدیریت سیستم های اساسی اینترنت شامل رمز نویسی و کد گذاری را به طور کامل کنترل کنند.

۲- خدمات وب رایانه خود را محفوظ نگه داشته و امنیت خود را جدی بگیرند.

۳- از دیواره آتش برای حمایت از شبکه خود استفاده نمایند.

۴- از ابزارهای کشف تجاوز و تخلف به منظور کشف حملات احتمالی استفاده نمایند.

۵- سیاست ها و روشهای مؤثری را برای اطمینان از بکارگیری بهترین روش انتصاب و در زمان مناسب استفاده کنند.

۶- تست های دوره ای برای کشف و کنترل شکاف ها و راه های نفوذ انجام دهند.

مدیران وکارکنان ممکن است، کارشناسان فن آوری اطلاعاتی نباشند، اما با این حال باید بدانند که جرائم اینترنتی تا چه حد می تواند خطرناک باشد و چگونه می توان به حفاظت از شرکت ها پرداخت.

جرائم اینترنتی امروزه همه را تهدید می کنند و زمان آن فرا رسیده است که خود را برای آینده آماده کنیم.

واژگان کلیدی:

فن آوری اطلاعات، پروتکل انتقال داده ها، امنیت شبکه اطلاعاتی، امضاء الکترونیکی، دیوارهای آتش، کدهای مخصوص مدیران، فن آوری وب، حملات اینترنتی، سرقت اطلاعات، ویروس رایانه ای، ماتریس جرائم اینترنتی، بیمه جرایم اینترنتی.

منبع فارسی :

تازه های جهان بیمه شماره ۵۴، آذر ۱۳۸۱.

منبع انگلیسی:

Asia Insurance Review Jun 2002

توضیحات:

۱. دیوار آتش نام نرم افزاری است که وظیفه کنترل و جلوگیری از دسترسی به اطلاعات شخصی را در شبکه کامپیوتری شرکت سرویس دهنده بر عهده دارد. (مترجم)