به نام خدا

ایمن‌سازی سازمان و تداوم کسب‌وکار

مؤلفین:

ندا غفوری فرد

راضیه سید مؤمن

سرشناسه	:	غفوری‌فرد، ندا، ۱۳۶۱ -
عنوان و نام پدیدآور	:	ایمن‌سازی سازمان و تداوم کسب‌وکار/مؤلفین ندا غفوری‌فرد، راضیه سیدمؤمن.
مشخصات نشر	:	تهران: آتی‌نگر، ۱۳۹۱.
مشخصات ظاهری	:	۱۰۴ص.: مصور، جدول، نمودار.
شابک	:	۴۸۰۰۰ ریال: ۸-۵۱-۶۰۰۴-۶۰۰-۹۷۸
وضعیت فهرست نویسی	:	فیپا
یادداشت	:	واژه نامه.
یادداشت	:	کتابنامه: ص. [۱۰۳- ۱۰۴].
موضوع	:	کامپیوترها -- ایمنی اطلاعات -- مدیریت
موضوع	:	کسب و کار -- منابع شبکه کامپیوتری
شناسه افزوده	:	سیدمومن، راضیه، ۱۳۵۵ -
رده بندی کنگره	:	۱۳۹۱ ۹ الف ۷غ/۷۶/۹ QA
رده بندی دیویی	:	۰۰۵/۸
شماره کتابشناسی ملی	:	۳۰۲۸۷۱۱

انتشارات آتی‌نگر

عنوان: ایمن‌سازی سازمان و تداوم کسب‌وکار

مؤلف: ندا غفوری‌فرد، راضیه سیدمؤمن

صفحه‌آرایی و طراحی جلد: همتا بیداریان

ناشر: آتی‌نگر

تیراژ: ۱۰۰۰

چاپ دوم: ۱۳۹۳

قیمت: ۴۸,۰۰۰ ریال

شابک: ۸-۵۱-۶۰۰۴-۶۰۰-۹۷۸

تلفن مرکز پخش: ۸-۶۶۵۶۵۳۳۶

آدرس: تهران- خیابان جمال‌زاده جنوبی- روبه‌روی کوچه رشتچی- پلاک ۱۴۴- واحد ۲

www.ati-negar.com

فهرست مطالب

فصل هشتم: ممیزی و مدیریت ریسک

فصل نهم: مباحث مدیریتی

پیوست: نکات مهم کتاب

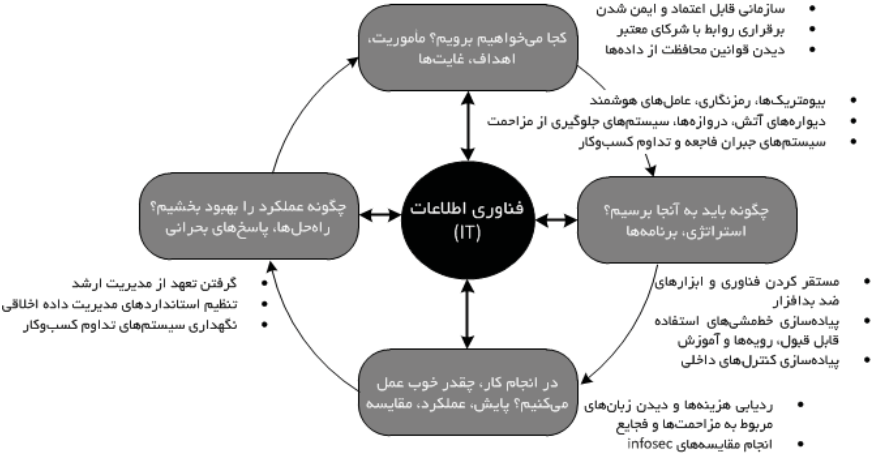
مقدمه

مدل عملکرد IT

زیان‌ها و اختلالاتی که به دلیل نادیده گرفتن امنیت IT به وجود می‌آیند می‌توانند به‌طور جدی از نظر مالی و عملیاتی به یک شرکت زیان برسانند یا آن را ورشکست کنند. از آن‌جایی که اثربخشی فناوری و تاکتیک‌ها توسط بزهکاران سایبری مورد استفاده قرار می‌گیرند (افرادی که با استفاده از اینترنت جرمی مرتکب می‌شوند)، بنابراین هزینه‌های مقابله با حملات حساب شده، ویروس‌ها و سایر نفوذهای بدافزار و خطاهای غیرعمدی افزایش می‌یابد. مدیران مسئولیت حفاظت از داده‌های محرمانه‌ای را که جمع‌آوری و ذخیره می‌کنند، برعهده دارند. اکنون طبق تحقیق صورت گرفته توسط Computer Economics (به آدرس computerconomics.com)، بسیاری از شرکت‌های کوچک و بزرگ در سرمایه‌گذاری در زمینه مدیریت امنیت حتی با بهترین اقدامات نظیر آموزش امنیت IT به کارمندان خود یا بررسی کامپیوترها جهت تضمین این که محتوا یا برنامه‌های غیرمجاز وجود ندارند، با شکست مواجه شده‌اند. شرکت‌ها برای تبعیت از قوانین فدرال، ایالتی و خارجی، باید در زمینه امنیت IT برای حفاظت از داده‌های خود، سایر دارایی‌ها، قابلیت انجام کار و درآمد شبکه سرمایه‌گذاری کنند (شکل ۱).

نفوذ به داده‌های ۵۵ میلیون دلاری در ChoicePoint

شرکت ChoicePoint یک دلال پیشرو در زمینه داده‌ها و خدمات اعتباری به شمار می‌رود. این شرکت ۱۹ میلیارد رکورد عمومی در مورد بیش از ۲۲۰ میلیون شهروند آمریکایی را نگهداری می‌کند. این شرکت داده‌های شخصی از جمله اسامی، شماره‌های امنیت اجتماعی، تاریخ تولدها، داده‌های شغلی و سوابق اعتبار را خریداری کرده و سپس داده‌ها را به مؤسسات تجاری و آژانس‌های دولتی می‌فروشد. بازاریابی، منابع انسانی، حسابداری و بخش‌های مالی برای مدیریت مشتری، بررسی سوابق و تأییدیه بر داده‌های ChoicePoint متکی هستند. به‌طور کلی، ۷۰ درصد درآمد ChoicePoint با فروش رکوردهای مصرف‌کننده برای تأیید حق بیمه و نمایش وضعیت محل کار به دست می‌آید.



شکل ۱- چرخه مدیریت عملکرد کسب‌وکار و مدل IT

ChoicePoint با نادیده گرفتن خط‌مشی خود در بررسی مجاز بودن مشتریان قبل از فروش داده‌ها، داده‌ها را در معرض ریسک قرار می‌داد. این مسأله قابل پیش‌بینی بود. در اوایل سال ۲۰۰۰، ChoicePoint بدون بررسی کافی سابقه، حساب‌های مشتریان را در اختیار هکرها قرار داد که برای دستیابی غیرقانونی به پایگاه‌های داده و سرقت داده‌های محرمانه مورد استفاده قرار گرفتند. در ماه می سال ۲۰۰۸، شرکت به علت نقض امنیت مجبور به پرداخت ۵۵ میلیون دلار جریمه شد، همچنین درصدد جبران سرقت هویت قربانیان، حل و فصل دعواهای حقوقی و پرداخت هزینه‌های قانونی برآمد. سپس در ژوئن ۲۰۰۸، این شرکت ۱۰ میلیون دلار بابت حل و فصل یک دادخواهی گروهی پرداخت کرد.

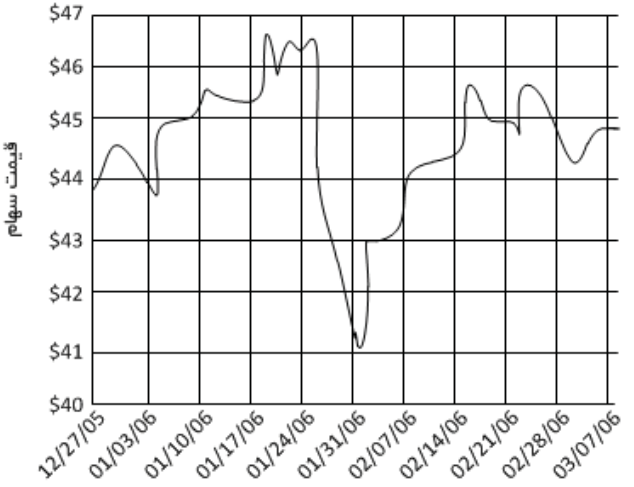
افشای مشکل در بین عموم

در ۱۵ فوریه سال ۲۰۰۵، شرکت ChoicePoint گزارش کرد که داده‌های شخصی و مالی ۱۴۵,۰۰۰ نفر "افشا" شده است. تمام این افراد در ریسک سرقت هویت بودند و این وضعیت پس از این روی داد که یک تبعه نیجریایی به نام Olatunji Oluwatosin که در کالیفرنیا زندگی می‌کرد، ادعا کرده بود معاملات تجاری مشروع متعددی را معرفی می‌کند.

عجیب آن که صلاحیت این فرد تأیید نشده بود و او ادغان داشت می‌تواند بیش از ۵۰ حساب جعلی ایجاد کند. این حساب‌ها امکان دستیابی او به پایگاه‌های داده حاوی داده‌های مالی و شخصی را فراهم می‌کردند. Oluwatosin در فوریه ۲۰۰۵، دستگیر شد و به جرم خود در مورد نقشه‌ای سری و سرقتی بزرگ اعتراف کرد و به ۱۰ سال زندان و پرداخت ۶/۵ میلیون دلار جریمه محکوم شد. جریمه‌های ایالتی و فدرال که برای شرکت ChoicePoint در نظر گرفته شد، بسیار بیش از این بود.

قوانین مربوط به حریم خصوصی و ضد کلاهبرداری، شرکت ChoicePoint را ملزم می‌کرد تا آنچه را که اتفاق افتاده بود افشا کند. قانون نقض حریم خصوصی کالیفرنیا مستلزم این است که وقتی اطلاعات شخصی برملا شدند، ساکنان شهر از این امر مطلع شوند. Outraged Attorneys General در ۱۴۴ ایالت درخواست کرد که شرکت به تمام شهروندان ایالات متحده که از این بابت صدمه دیده‌اند، اطلاع دهد. در سطح فدرال، شرکت ChoicePoint به چند فقره اهمال کاری و شکست در زمینه پیگیری اقدامات معقول امنیت اطلاعات متهم شد. در سال ۲۰۰۵، این شرکت با پرداخت جریمه‌ای سنگین در Federal Trade Commission (FTC) یعنی ۱۵ میلیون دلار مواجه شد. FTC شرکت ChoicePoint را در موارد زیر به تخلف محکوم کرد:

- ✓ Fair Credit Reporting Act (FCRA) برای جلب اطمینان، گزارش‌هایی به مشترکانی که مجوز دریافت آن‌ها را ندارند ارسال می‌کند و همچنین عدم رعایت قوانین منطقی برای بررسی هویت مشترکان خود
- ✓ FTC Act برای اظهارات دروغین و نادرست درباره خط‌مشی‌ها حریم خصوصی در وب‌سایت خود
- ✓ در ۴ مارس ۲۰۰۵، زمانی که شرکت برای اولین بار چنین اقدامی کرد، یک گزارش 8-k برای سهامداران تهیه کرد که درآمد آن‌ها به علت نفوذ به داده‌ها تحت‌الشعاع قرار گرفته بود. در ژانویه ۲۰۰۶، شرکت فوق با اعلان عمومی میزان جریمه‌ها، افت قیمت موجودی را اذعان داشت که در شکل ۲ نشان داده شده است.



شکل ۲- تأثیر نفوذ در داده‌ها بر قیمت سهام شرکت ChoicePoint

راه‌حل

وقتی یک شرکت قوانین SEC، فدرال یا ایالتی را نقض می‌کند، راه‌حل مشکل به آن‌ها دیکته می‌شود. راه‌حلی برای جلوگیری از به ریسک افتادن ChoicePoint توسط FTC ارائه شد. این شرکت باید رویه‌های جدید را اعمال می‌کرد تا تضمین کند که مصرف‌کننده فقط به مؤسسات تجاری مجاز در مورد مقاصد قانونی گزارش می‌دهد. علاوه بر این، FTC به شرکت ChoicePoint دستور داد برنامه امنیت اطلاعات جامعی را ایجاد و نگهداری کند و ممیزی‌ها را توسط افراد حرفه‌ای شرکت‌های مستقل دیگر هر دو سال یکبار تا سال ۲۰۲۶ تهیه کند. ChoicePoint برای جلب اطمینان ذی‌نفعان، Carol DiBattiste، معاون سابق Transportation Security Administration را به عنوان مدیر ارشد CPO استخدام کرد.

نتایج

ChoicePoint فعالیت‌های خود در زمینه کسب‌وکار و معیارهای امنیت داده‌ها را که خیلی آسان در معرض ریسک قرار می‌گرفتند، اصلاح کرد. این شرکت باید فعالیت‌های

تجاری پر ریسکی را که بر درآمدهای کوتاه مدت پیش از سوددهی طولانی مدت متمرکز شده بود، متوقف می‌کرد. این تصمیم‌گیری ضروری و کاملاً اخلاقی است.

نفوذ به داده‌های ChoicePoint توجه عامه مردم را به خط‌مشی‌های امنیت بنگاه‌ها جلب کرد. این امر نیاز به حاکمیت سازمانی بهبودیافته (به آدرس corpgov.net) را نشان می‌داد. هر چند تعریف قابل قبولی در این مورد وجود ندارد، ولی **حاکمیت سازمانی**[۱] به قوانین و رویه‌هایی اشاره دارد که تضمین می‌کنند سازمان از استانداردهای اخلاقی قابل قبول، بهترین اقدامات و قوانین پیروی می‌کند. شرکت‌هایی که اطلاعات حساس مصرف‌کنندگان را جمع‌آوری می‌کنند، مسئول هستند که آن‌ها را در جای امنی نگه دارند. کلاهبرداری‌های سطح بالا و بدافزار و نفوذ در داده‌ها باعث افزایش درگیری‌های دولت و پلیس برای مسئول‌پذیر کردن شرکت‌ها و مدیریت آن‌ها در قبال اشتباهات خود می‌شود. ولی به دلیل نفوذ در داده‌های ثبت شده ChoicePoint، حوادث امنیت اطلاعات و سرقت داده‌های متعددی روی داد.

منابع: برگرفته از ftc.gov، Gross (2005)، Kaplan (2008)، Mimo (2006) و Scalet (2005).

درس‌هایی که از این مورد می‌توان آموخت

هر سازمانی از اطلاعات ارزشمندی برخوردار است که جنایتکاران در سراسر دنیا تلاش می‌کنند آن‌ها را سرقت کنند. ریسک‌ها امنیت IT، ریسک‌ها کسب‌وکار هستند. امنیت فناوری اطلاعات[۲] (IT) به حفاظت از اطلاعات، شبکه‌های ارتباطاتی و عملیات قدیمی و تجارت الکترونیکی جهت تضمین محرمانگی، صحت، قابلیت دسترسی و کاربرد مجاز اشاره دارد. هدف این است که در برابر ریسک عملیاتی و بی‌نظمی، زیان مالی و بدهی، از مصرف‌کنندگان زیان‌دیده دفاع شود. **ریسک عملیاتی**[۳]، ریسک هر زیانی است که از فرآیندهای داخلی ناقص یا نامناسب، افراد، سیستم‌ها یا رویدادهای خارجی حاصل می‌شود. امنیت فناوری اطلاعات (IT) به قدری با اهداف کسب‌وکار یکپارچه است که نمی‌تواند به

[1]- Corporate Governance
[2]- IT Security
[3]- Operational Risk

عنوان یک کارکرد مستقل رفتار کند. شکست‌ها تأثیر مستقیمی بر عملکرد کسب‌وکار، مشتریان، شرکای کسب‌وکار و ذی‌نفعان دارند.

در این کتاب، با بررسی مشکلات امنیتی سازمان‌ها شروع می‌کنیم. درباره فناوری‌هایی نظیر دیواره‌های آتش و بدافزار، کنترل‌های داخلی، بیمه و چارچوب کاری COBIT بحث می‌کنیم. یک مدل نمایشی ریسک را برای آشنایی با آنچه که باید حفاظت شود و میزان سرمایه‌گذاری در این زمینه معرفی می‌کنیم. تهدیدهای اصلی و انواع کلاهبرداری‌ها را شرح می‌دهیم و این که چگونه آن‌ها باعث افزایش و شیوع اسپم، بات‌ها و Phishing می‌شوند. توجه داشته باشید که از اصطلاح امنیت اطلاعات (یا به اختصار infosec) برای اشاره به امنیت داده‌ها، شبکه‌ها، برنامه‌های کاربردی، ارتباطات و هر مورد دیجیتالی دیگری که سازمان برای فعالیت خود به آن نیاز دارد، استفاده می‌کنیم.