با مدیریت جامع اطلاعات (EIM[1])، از اطلاعات خود محافظت کنید.

یکی از بزرگترین نگرانی های واحد انفورماتیک هر سازمان در همه جای دنیا امنیت اطلاعات(Information Security) است. هفته ای نیست که داستانی از شکسته شدن سیستم امنیت اطلاعات سازمانی شنیده نشود. از سوء استفاده‌های داخلی وحمله‌ی هکرها گرفته تا جاسوسی سازمانهای رقیب و جنگ‌های سایبری حساس بودن این موضوع و حضور خطر برای هر سازمانی را نشان می دهد.

جمع بندی:

با راه‌حل های امنیت اطلاعات سازمان شما می‌تواند:

- از امنیت جامع اطلاعات و پوشش و ساماندهی و اختصاص دهی اطلاعات اطمینان یابد.
- کنترل مجوز ها در استفاده از اطلاعات بسیار مهم سازمانی را کنترل کند.
- تاریخچه‌ی کسانی در بین سازمان به اطلاعات دسترسی دارند را ردگیری و ثبت کند.
- اطلاعات و دارایی های دانشی را محافظت کند.
- تبادل اطلاعات موثر و کارآمدتر بین افراد درون سازمانی و برون سازمانی مجاز را تسهیل کند.
- در فرآیند ها و نرم افزارهای سازمان بدون لطمه زدن به امنیت آنها، اطلاعات را یکپارچه سازی کند.

حفاظت از اطلاعات می تواند روی کیفیت و جریان اطلاعات مورد نیاز اعضای هر سازمان اثر بگذارد. ایجاد تعادل بین حفاظت و بهره‌وری، کلید ساختاری در امنیت اطلاعات است. به عبارت دیگر، تبادل اطلاعات، هم ریسک و هم ارزش ایجاد می کند. سازمان‌ها با هم رقابت می کنند، ولی ما در دنیای «ویکی لیکس»ها زندگی می‌کنیم. تهدید افتادن اطلاعات به دست افراد غیرمجاز، محتمل و دارای عواقب جدی است. لو رفتن اطلاعاتی از جنس مالی، حقوقی، فنی و غیره باعث از دست دادن مالکیت معنوی و مزیت رقابتی می‌شود و می‌تواند آسیب بسیاری به شهرت، نام تجاری و بنیاد سازمان وارد کند.

راه حل این نیست که همه‌ی اطلاعات بسته شوند طوریکه نتوان آن‌ها را خواند و یا به اشترک گذارد. چرا که کنترل بیش از حد امنیتی هم در فرآیندهای سازمانی اخلال ایجاد می کند و هم می‌تواند همانند یک کنترل ناقص و مضر باشد.

هر سازمان باید بتواند راه حلی برای به تعادل رساندن آن بیابد. در برخی موارد اعمال کنترل بسیار دقیق بر اطلاعات با اولویت بالا مانند فرمول داروها، طراحی تجهیزات نظامی و یا امنیتی، ضروری است. در دیگر موارد نیاز است که حرکت آزاد و روان اطلاعات بین گروه‌ها و شرکای تجاری و افراد سازمان وجود داشته باشد. راه حل پیشنهادی شرکت ایران رایانه، استفاده از مدیریت جامع اطلاعات (EIM) و هوشمند سازی امنیت فن‌آوری اطلاعات و ایجاد آگاهی از ریسک های اجرایی است.

(۱) Enterprise Information Management

امنیت اطلاعات در طراحی کلی محصولات و راه‌حل‌های ایران رایانه پیاده‌سازی شده است. مدیریت جامع اطلاعات (EIM)، امنیت اطلاعات، محتوا و فرآیندهای کاری در کل سازمان را تامین می‌کند. EIM این امکان را برای کاربران سازمان فراهم می آورد که بتوانند بدون ایجاد خط و مرز برای مشخص کردن مکان و روش استفاده در داخل یا خارج سازمان، شخص یا اشخاصی را که می‌بایست به اطلاعات دسترسی داشته باشند، انتخاب کنند.

چه زمانی شما به امنیت اطلاعات احتیاج دارید؟

امنیت اطلاعات برای دو وضعیت در نظر گرفته می‌شود: اطلاعات ساکن (بایگانی) و اطلاعات در حال حرکت. بین این دو تفاوت‌های مهمی وجود دارد که بایستی در هر سازمان بررسی و شناخته شود.

اطلاعات ساکن: امنیت اطلاعات درون سازمانی

حفاظت اطلاعات ذخیره شده روی سرورهای داخلی سازمان، سر راست و ساده تر از حفاظت اطلاعات در حال حرکت است. ارائه‌ی رمزگذاری قوی و تصدیق هویت برای مخزن نگهداری فایل‌های الکترونیک تضمین می‌کند که فقط کارمندان و نرم افزارهای مجاز، اجازه‌ی دسترسی به محتوا را داشته باشند. در سطوح امنیتی ممکن است داده‌های اطلاعاتی با توجه به مرحله‌های مختلف، نیاز به تغییر سطح دسترسی اشخاص و نرم‌افزارهایی باشند که دارای مجوزند.

کنترل دسترسی بسیار دقیق(Granular Control) امکان ها و مجوزها نه فقط برای دسترسی به اطلاعات است بلکه اجازه‌ی جستجو را نیز می دهد. به این صورت که نتیجه‌ی جستجو نباید اطلاعاتی را در برگیرد که کاربر اجازه‌ی دسترسی به آنها را ندارد. به عنوان نمونه، در خدمات رسانه‌های اجتماعی خودکار، همانند ارسال های (مایکرو وبلاگینگ)، کاربر فقط امکان تغییر دادن بخشهایی از اطلاعات را دارد که عده‌ای خاص مجوز مشاهده‌ی آن را دارند. تاریخچه ممیزی، دسترسی اشخاص و زمان و رویدادهای مهم مربوط به اطلاعات را نشان می‌دهد. برخی اطلاعات، مانند اسناد الکترونیکی می‌بایست سال‌ها و دهه ها بایگانی شوند. به دلایل قانونی و یا نظارتی، گونه‌های مختلف محتوا باید برای همیشه قابل بازیابی باشند. برای محقق شدن امنیت مطمئن، حفاظت بلند مدت نوعی بیمه است که نه فقط برای ایجاد آرامش خاطر ذینفعان سازمانی است، بلکه در درجه‌ی بالاتر منافع مهم مالی را در موقعیت های مختلفی مانند دعوا های حقوقی، اختلاف های ثبت اختراعات و یا بلایای طبیعی حفظ می‌کند.

چگونگی ایجاد تعادل بین حفاظت و بهره وری، کلید ساختاری امنیت اطلاعات است.

اطلاعات در حرکت: امن کردن اطلاعات خارج از دیواره آتش

امروزه در ارتباطات و مشارکتهای قوی کسب و کار جهانی، اطلاعات سازمان نمیتواند در بین مرزهای فیزیکی سازمان باقی بماند. تنوع دستگاهها و مدل های مختلف ارتباطی (ایمیل، لپ تاپها، موبایلها، شبکه های ابری و...)، دیوارهای آتش هستند.

در عصر کنونی، هر سازمان باید امکان حفاظت از اطلاعات حساس را در همه جا داشته باشد، و این دور اندیشی وجود داشته باشد که اطلاعات ممکن است در هر زمان به دست اشخاص غیر مجاز بیفتد. به عنوان مثال، مذاکرات یک قرارداد را درنظربگیرید. در طول مذاکرات، اطلاعات بسیار محرمانه با یک مخاطب خارجی البته با حسن نیت رد و بدل می شود. ولی اگر مذاکرات قطع شود هریک از طرفین نگران فاش شدن اطلاعات خودمربوط با آن فرآیند هستند. بسیار این موقعیت اتفاق می افتد که افراد، دانسته یا نادانسته اطلاعات محرمانه را با افراد یا سازمانهای- داخلی یا خارجی و مجاز یا غیرمجاز- به اشتراک می گذارند. اغلب از طریق ایمیل و یا رسانه‌های اجتماعی این اتفاق می افتد. این معنی«اطلاعات در حرکت» است.

رمزگذاری SSL نخستین نیاز امنیتی اطلاعات در حرکت است که باید امنیت مسیر انتقال اطلاعات از سمت شخص، سیستم یا دستگاه به دیگری را پوشش دهد.ایجاد امنیت ایده‌آل نیازمند مدیریت صحیح مدل ها است، که چطور رفتار مناسبی در مقابل افتادن اطلاعات به دست افراد اشتباه، چه به صورت سهوی و یا عمدی داشته باشد. مدیریت صحیح، همچنین نقش موثری در کنترل اطلاعات خارج از مخزن سازمان و دسترسی آن به افراد قانونی و تایید شده را دارد.برای نمونه آنها ممکن است فقط مجوز خواندن، چاپ همراه با نشانه‌ی (Watermark) را داشته باشند و اجازه‌ی ارسال ایمیل نداشته باشند. این سطح امنیتی می تواند مسیر اطلاعات در فرآیند های سازمانی، انتشار در پورتال ها و وب سایت ها یا کانال های ارتباطی مشتریان و ... را نیز پوشش دهد.
با وجود تهدید ها، سرقت ها و خطرها می بایست اطلاعات در سازمان جریان داشته باشد. و در این میان امنیت اطلاعات برای حفظ مالکیت معنوی و داده های حساس سازمانی نقش بسیار حیاتی را ایفا می کند.

ارزش سازمانی امنیت اطلاعات

در ساده ترین شرایط، سازمان ها به سه دلیل در تکنولوژی سرمایه گذاری می کنند: هدایت ارزش کسب وکار، کاهش هزینه ها، کاهش خطرها. جای تعجب نیست که امنیت اطلاعات در اولویت اول برای کاهش خطر ها ولی برای تمامی موارد نام برده طراحی شده است.

با این حال، می توان حتی به نقش امنیت اطلاعات در کاهش اصطکاک بین فرآیند های سازمانی و همکاری اشاره کرد.برای توضیح این مورد: در جایی که ممکن است کارمندان سازمان های مختلف درگیر اشتراک اطلاعات بسیار حساس در طیف وسیعی از نرم افزارها، ابزارها و شبکه های متنوع باشند، امنیت اطلاعات مانند یک روان کننده، این فرآیند ها را بی دردسر در پشت صحنه مدیریت می کند. بدون این پوششها، همکاری ها آهسته تر و محدودتر صورت می گیرد، مانند جلسه های وقت گیر و پر هزینه‌ی افراد. با کاهش خطر، امنیت اطلاعات می تواند به چابکی سازمان و سرعت و نو آوری و رشد و تکامل آن کمک کند.

هرچند امنیت اطلاعات به عنوان هزینه‌ای برای کسب و کار دیده می شود ولی همچنین در بلند مدت نقش کاهش دهنده‌ی هزینه ها را بازی می کند. مانند هزینه‌ی کمی که برای بیمه در مقابل پیشگیری خسارات فجایع بزرگ پرداخت می شود. بنابراین امنیت اطلاعات نقش محافظ در مقابل آسیب ها به نام تجاری سازمان را ایفا می کند و از هزینه های سنگین ترمیم و باز سازی جلوگیری می کند.
علاوه بر این، اگر امنیت اطلاعات جزو راه حل های جامع مدیریت اطلاعات همانند فایلر باشد، بیشترین دستاورد در کمترین هزینه به دست خواهد آمد.

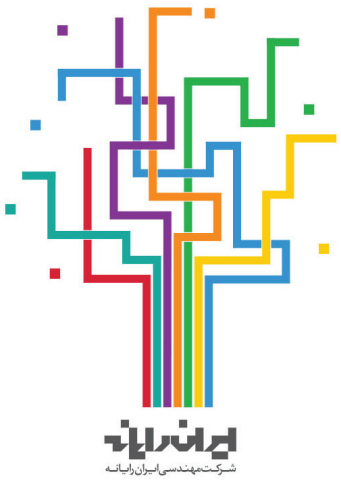
جمع بندی:

تا زمانی که داستانهای نفوذ امنیتی به شرکتها و سازمانهای دولتی به طور مکرر در اخبار دیده می‌شود امنیت اطلاعات در اولویت دپارتمانهای فن آوری اطلاعات میماند. اینکه چه اطلاعاتی «در حال سکون» یا «در حرکت» است، میباید در مقابل متجاوزان مانند کارمندان، مشتریان، رقبا و یا هرکس دیگری که اجازه دسترسی ندارد، محافظت شود.

با راه حل های جامع فایلر، امنیت اطلاعات برون سازمانی به خوبی امنیت اطلاعات درون سازمانی است.

راه حل های امنیت اطلاعات فایلر، به عنوان بخشی از استراتژی EIM، تعادل بین حفاظت و بهره وری را با اجازه دادن گردش امن اطلاعات در فرآیندهای کسب و کار است. فایلر، چه درون سازمان و چه خارج از آن، امکان خواندن، چاپ، دانلود و یا به اشتراک گذاری اسناد را فقط زمانی امکان پذیر می سازد که از صحت افراد تاییدشده مطمئن باشد.

فایلر مدیریت جامع اطلاعات
Enterprise Information Management



ایران رایانه
شرکت مهندسی ایران رایانه