ده اشتباه مرگبار در مدیریت امنیت اطلاعات

Hacked!
Shift
Home
PgUp
1
2
3

پیادهسازی یک برنامه مدون و منسجم مدیریت امنیت اطلاعات در هر سازمانی از اهمیت بسیاری برخوردار است. عدم توجه و رسیدگی به این مسئله دو پیامد مهم به همراه دارد . اول آنکه صدمههای جبرانناپذیری به سازمان وارد میکند و دادههای سازمان را در معرض خطر قرار میدهد و دوم آنکه باعث از دست رفتن اعتماد مشتریان به یک سازمان میشود . درنتیجه پیادهسازی یک استراتژی منسجم برای حفاظت از اطلاعات میبایست سرلوحه کار هر سازمانی قرار داشته باشد .

بر همین اساس در این مقاله تصمیم گرفتیم به شناسایی و بررسی 10 جنبه مهم و تأثیرگذار در طرحها و استراتژیهای حاکمیت امنیت اطلاعات بپردازیم . این اصول که درواقع، بنیان استراتژی امنیت اطلاعات را شامل میشوند، اگر بهدرستی پیادهسازی نشده یا تفسیر اشتباهی از آنها برداشت شود، نهتنها بزرگترین طرحهای امنیت سازمانی را با شکست روبرو میسازند، بلکه رخنههای امنیتی جدی را در برنامهریزیهای سازمانی به وجود میآورند . این 10 جنبه میتوانند بهعنوان یک فرم ارزشیابی توسط مدیران ارشد برای حصول اطمینان از تعریف یک برنامهریزی جامع و تأثیرگذار مورداستفاده قرار گیرند . این مقاله ماحصل سالها آموزش امنیت اطلاعات به طیف گستردهای از مخاطبان و همچنین مشاوره در پروژههای امنیت اطلاعات در بسیاری از شرکتها است . این مقاله ازآنجهت 10 اشتباه مرگبار مدیریت امنیت اطلاعات لقب گرفته است که در صورت عدم توجه به آنها میتوانند در زمان پیادهسازی یک پروژه موفقیتآمیز آن را دستخوش بحرانهای شدیدی کنند .

مطلب پیشنهادی

5 علامت_هشداردهنده هک_شدن یک برنامه وب

1. عدم درک این موضوع که امنیت اطلاعات یک مسئولیت سازمانی است

این نکته را به یاد داشته باشید که حاکمیت امنیت اطلاعات، یک بخش ضروری و یکپارچه در حاکمیت سازمانی به شمار میرود . این موضوع در سالهای اخیر اهمیت بیشتری پیدا کرده است . بهطوریکه به یک قانون بینالمللی تبدیلشده و حتی درباره مواردی الزامات قانونی را در سطح جهانی به وجود آورده است. برآیند این قوانین باعث میشوند تا حریم خصوصی مشتریان و بهطور مثال دادههای مربوط به بیماران تحت لوای این قانون قرارگرفته و حریم خصوصی مشتریان بیشازپیش خصوصیتر باقی بماند . بر همین اساس بعضی از دولتها قوانینی را در این زمینه اتخاذ کرده و سازمانها را ملزم به اجرای آنها ساختهاند . ازجمله این قوانین و پیشنیازهای قانونی میتوان به King II Report در آفریقای جنوبی، SA، ECT Act و HIPPA Act (HIPPA) در ایالاتمتحده اشاره کرد .

تفسیر ساده تحولات به وجود آمده اینگونه است که هیئتمدیره و مدیران ارشد سازمانها مسئولیت مستقیم اداره امور سازمان را بر عهده خواهند داشت و نسبت به حفظ تمام داراییهای اطلاعاتی یک سازمان به شیوه ایمن مسئول خواهند بود . این قوانین نهتنها مدیران را مقید میسازند که درزمینه حفظ امنیت و محافظت از داراییهای اطلاعاتی سازمان باید به شیوهای ایمن و مسئولانه رفتار کنند، بلکه آنها را ملزم میکنند که تدابیر لازم را برای حفظ امنیت اطلاعات به کار گرفته و برای ایمن نگهداشتن اطلاعات کاربران بیوقفه در تلاش و کوشش باشند . بیتوجهی به این قوانین نهتنها باعث به خطر افتادن داراییهای اطلاعاتی سازمان شده و تبعات مالی را برای سازمان به همراه دارد، بلکه مشکلات حقوقی و قانونی جدی را برای سازمانها به همراه خواهد آورد . این قوانین بهصراحت اعلام میکنند که مدیران اجرایی مسئول بروز هرگونه مشکل امنیتی در این زمینه هستند .

علاوه بر این، مدیر اجرایی مسئولیت دیگری را بر عهده دارد؛ او موظف است گزارش محافظت از داراییهای اطلاعاتی سازمان را بهطور منظم و مشروح در اختیار هیئتمدیره قرار دهد . درصورتیکه مدیران اجرایی آنگونه که از آنها انتظار میرود در این زمینه تلاشهای لازم را انجام نداده و در این زمینه سهلانگاری کرده باشند، تعهدات فردی خود و سازمان مطبوع خود را در معرض مشکلات جدی قرار خواهند داد .

2. عدم درک این موضوع که حفاظت از اطلاعات بیش از آنکه یک مسئله فنی باشد یک موضوع تجاری است

این اشتباه ارتباط تنگاتنگی با اشتباه اول داشته، اما چالش خاص خود را دارد، به دلیل اینکه از زاویه دیگری مشکلساز میشود . مشکلات امنیتی یک سازمان تنها با ابزارهای فنی حل نمیشوند . اگر مدیر سازمانی در اسرع وقت مشکل را شناسایی کند، به همان نسبت در سریعترین زمان ممکن توانایی ارائه راهحل مربوطه را خواهد داشت؛ اما متأسفانه، در بسیاری از موارد، مدیران اجرایی در سازمانها بر این باور هستند که فناوری علاج همه مشکلات است، درنتیجه نهتنها مشکل را به دپارتمان فنی شرکت واگذار میکنند، بلکه مسئله را کماهمیت در نظر گرفته و بهسرعت آن را فراموش میکنند . اگر حمایت مناسب، مستقیم و مستمر مدیر اجرایی وجود نداشته باشد و همچنین سطح آگاهی درزمینه مشکل امنیتی کم باشد، مشکل امنیتی آنگونه که باید بهطور رضایت بخشی حل نخواهد شد . بیتوجهی به این مشکل باعث میشود، فناوری به امنیت اطلاعات وارد شود، اما در عمل هیچگونه راهحل جامعی برای برونرفت از مشکل ارائه نکند . درنتیجه سرمایههای یک سازمان بهراحتی از دست میروند .

3. عدم درک این موضوع که حاکمیت در بحث امنیت اطلاعات یک قاعده چندبعدی است

امنیت اطلاعات رشتهای چندبعدی از فاکتورهای متعدد است . اگر در نظر دارید سنگ بنای یک محیط ایمن و مناسب را پایهریزی کنید که از همه داراییهای اطلاعاتی یک سازمان محافظت به عمل آورد، باید همه جنبههای امنیتی مرتبط با یکدیگر را موردتوجه قرار دهید . بهعبارتدیگر باید مؤلفههای مختلف موردبررسی قرار گیرند . امنیت اطلاعات ابعاد مختلفی را شامل میشود که از آن جمله میتوان به بعد

(Organizational Dimension) (Corporate Governance Dimension)
Best Practice) (Policy Dimension)
(Dimension (Ethical Dimension)
(Legal dimension) (CertificationDimension)
(Awareness Dimension) (Personnel/HumanDimension)
(Technical Dimension) (Measurement/Metrics Dimension)
(Audit Dimension).

4.

5.

.

.

.



است

اگر امکان نظارت و پیروی از سیاستهای اتخاذ شده در یک سازمان امکانپذیر نباشد، داشتن یک سیاست امنیت اطلاعاتی جامع در یک سازمان یا حتی برخورداری از سیاستهای خرد حمایتی و پیروی از الگوهای بینالمللی هیچگونه سودی به همراه نخواهد داشت . درصورتیکه سیاستهای اتخاذ شده قابلیت اجرا نداشته باشند خود عاملی برای بروز اختلال خواهند شد . مدیران امنیت اطلاعات باید بتوانند فارغ از مباحث فنی توانایی بازرسی و نظارت بر روند اجرای برنامههای امنیتی را داشته باشند و اگر بخشی از یک سازمان از این سیاستها پیروی نکرد، توانایی اتخاذ تصمیمهای لازم برای بخش مربوطه را داشته باشند . این بازرسیها که اغلب با ابزارهای نظارت و سنجش انجام میشوند نباید بر مبنای گزارشهای حسابرسی باشند که بهصورت سالیانه یا دوسالانه ارائه میشود . بهطور مثال آیا کارمندی که شش ماه از اخراجش گذشته است هنوز به سیستم دسترسی دارد یا خیر. ابزارهای نظارتی باید توانایی ارائه گزارشهای لحظهای را داشته باشند . این ابزارها همچنین باید بهگونهای طراحیشده باشند که بهطور مستقیم به سراغ اشتباه رخداده بروند تا مدیریت آن بهآسانی امکانپذیر باشد . اگر این سیاست بهاشتباه تفسیر شود، این ذهنیت را به وجود میآورد که ما همه سیاستهای لازم را به مرحله اجرا گذاشتهایم؛ اما در عمل دامنه اشتباهات بهمرورزمان گستردهتر شده و همچنین پیروی از الگوهای سیاستی نیز به دست فراموشی سپرده خواهند شد.

8. عدم درک این موضوع که پیادهسازی یک ساختار متناسب برای حاکمیت امنیت اطلاعات امری ضروری است

شرط لازم برای پیادهسازی یک طرح حاکمیت امنیت اطلاعات این است که سازمان از یک ساختار سازمانی مناسب برای این منظور تبعیت کند . این ساختار باید توجه ویژهای به نحوه سازماندهی و اجرای امنیت اطلاعات داشته باشد . پیادهسازی این ساختار توسط بسیاری از استانداردها برای مدیریت اطلاعات تأیید شده است. دستورالعملهای جهانی امنیت نشان میدهند که وجود یک ساختار سازمانی مناسب به معنای یک مرکز مشاوره برای امنیت اطلاعات ایفای نقش میکند و باعث میشود الگوی امنیت اطلاعات با موفقیت

در یک سازمان پیادهسازی شود. این بُعد نهتنها ساختار را موردتوجه قرار میدهد، بلکه به جنبههایی همچون مسئولیتهای شغلی مرتبط با امنیت اطلاعات، ارتباط بین وظایف مرتبط با امنیت اطلاعات و مشارکت مدیران ارشد در امنیت اطلاعات نیز رسیدگی میکند . در این ساختار مشخص میشود کدام جنبههای مدیریت امنیت اطلاعات متمرکز و کدام جنبهها از درجه اهمیت کمتری به لحاظ متمرکز بودن برخوردار هستند. همچنین بهوضوح نشان میدهد در کدام بخشها باید نظارت، اجرا و پیروی از قوانین موردتوجه قرار گیرد . عدم توجه به این مسئله باعث میشود همه مشکلات امنیتی بهطور مستقیم به دست مدیر امنیت اطلاعات سپرده شود، درحالیکه مدیر امنیت مالک این اطلاعات نیست بلکه نقش یک متصدی را بر عهده دارد . اگر در ساختار امنیت اطلاعات، مالکیت اطلاعات بهدرستی تعریف نشود و افراد اطلاع نداشته باشند که در صورت افشای اطلاعات، آنها مسئول به خطر افتادن امنیت اطلاعات خواهند بود، آنگاه مخاطرات امنیتی بزرگی به وجود خواهد آمد . همچنین مسئولیتپذیری در ارتباط با امنیت اطلاعات باید در قالب یک وظیفه اشتراکی توسط همه کارکنان موردتوجه قرار گیرد . نه اینکه همه این موارد جزء مسئولیتهای مدیر امنیت اطلاعات در نظر گرفته شود . این مسئله نهتنها باید بهصورت شفاف نشان داده شود بلکه باید بهدرستی در چارت اصلی سازمان تعریفشده باشد .

9. عدم درک این موضوع حیاتی که سطح آگاهی کاربران از امنیت اطلاعات باید افزایش یابد

هرچند این اشتباه کاملاً مشخص و روشن است و نیازی به هیچگونه توضیحی ندارد . در بسیاری از سازمانها هیچگونه برنامهای برای آگاهسازی صحیح کاربران وجود ندارد . بهطوریکه در بسیاری از موارد کاربران از ریسکهایی که پیرامون زیرساختهای مورداستفاده توسط آنها قرار دارد، هیچگونه اطلاعی ندارند . در بعضی از سازمانها کاربران حتی از سیاستگذاریهای امنیت اطلاعات و استانداردهایی که در شرکت تعریفشده است، نیز هیچگونه اطلاعی ندارند . اگر برای کاربران توضیح داده نشود که مشکلات امنیتی چه مشکلاتی هستند و برای پیشگیری از بروز آنها چه اقداماتی باید انجام شود، در صورت بروز مشکلات امنیتی نمیتوان آنها را مقصر دانست . بهطورکلی پولی که برای اطلاعرسانی جامع در ارتباط با افزایش سطح آگاهی کاربران مصرف میشود در مقایسه با پولی که صرف امنیت اطلاعات میشود بیشتر است، اما در غایت از بروز صدمات جبرانناپذیر جلوگیری به عمل میآورد .

10. غافل شدن مدیران امنیت اطلاعات از زیرساختها، ابزارها و سازوکارهای حمایتی که برای اجرای مسئولیتهای خود به آنها نیاز دارند

این اشتباه ارتباط مستقیمی با اشتباهات شماره هفت و هشت دارد؛ اما بهعنوان یک مشکل اساسی موردتوجه قرار میگیرد . بسیار دیدهشده است که در سازمانها مدیران اجرایی فردی را بهعنوان مدیر امنیت اطلاعات تعیین میکنند و از او انتظار دارند تا همه مسائل مرتبط با امنیت اطلاعات را موردبررسی قرار دهد؛ اما در عمل به دلیل پیچیده بودن مکانیسمها و چندبُعدی بودن امنیت اطلاعات این کار امکانپذیر نیست . اتخاذ چنین الگویی باعث میشود، مدیران امنیت اطلاعات بهسرعت به این واقعیت آگاه شوند که توانایی انجاموظیفه خود را ندارند و رفتهرفته کنترل امنیت اطلاعات از دست آنها خارج میشود . این موضوع باعث میشود تا سازمان در معرض مخاطرات امنیتی جدی قرار گیرد، به این دلیل که پیوستگی درروند کنترل موضوعات وجود نخواهد داشت . درنتیجه برنامه امنیتی هیچگاه بهطور کامل پیادهسازی نخواهد شد

============================

شاید به این مطالب هم علاقمند باشید :

حسگرهای اثر انگشت عامل افزایش امنیت یا کاهش امنیت؟!

رمزنگاری اطلاعات بیهوده است؛ شما باز هم هک میشوید

به این چهار نکته توجه کنید تا هک نشوید!

5 علامت هشداردهنده هک شدن یک برنامه وب

The site ahead contains harmful programs

Attackers on [redacted] might attempt to trick you into installing programs that harm your browsing experience (for example, by changing your homepage or showing extra ads on sites you visit).

☐ Automatically report details of possible security incidents to Google. Privacy policy

Details
Back to safety

[ضمان حماية الكمبيوتر من الفيروسات والبرامج الضارة]

[ضمان حماية الكمبيوتر من الفيروسات والبرامج الضارة (برنامج مجاني)]

[برنامج الحماية من الفيروسات والبرامج الضارة]

[**10** برنامج الحماية من الفيروسات والبرامج الضارة]

چگونه از خودمان در برابر تبلیغات مخرب محافظت کنیم؟

مترجم:
حمیدرضا تائبی
منبع :
الزویر
دسته بندی:
امنیت
تاریخ انتشار :
11:50 - 16/12/1394
برچسب:
امنیت فناوری اطلاعات - مدیریت امنیت اطلاعات - امنیت اطلاعات

□□□□□ منبع :https://www.shabakeh-mag.com/security/3020