راهنمای امنیت سایبری کسب‌وکارها در بحران

معاونت مطالعات اقتصادی و آینده‌پژوهی

اتاق بازرگانی، صنایع، معادن و کشاورزی تهران

بسم الله الرحمن الرحیم

تهران؛ پایتخت تجارت ایران

معاونت مطالعات اقتصادی و آینده‌پژوهی

اتاق بازرگانی، صنایع، معادن و کشاورزی تهران

راهنمای امنیت سایبری کسب‌وکارها در بحران

مرداد ۱۴۰۴

از طریق پست الکترونیکی زیر می‌توانید پیشنهادها و نظرات اصلاحی خود را به واحد مربوطه منعکس کنید:

Economic_research@tccim.ir

فهرست مطالب

عنوان صفحه

مقدمه

بحران‌هایی مانند جنگ، حملات تروریستی، ناآرامی‌های سیاسی یا حملات زیرساختی نه‌تنها امنیت فیزیکی بلکه بنیان دیجیتال و اطلاعاتی کسب‌وکارها را نیز به‌شدت تحت تأثیر قرار می‌دهند. در چنین شرایطی، حفظ امنیت اطلاعات، حریم خصوصی داده‌ها و تداوم عملیات سازمانی فقط یک انتخاب اختیاری نیست. در واقع امنیت دیجیتال در بحران، ضرورتی حیاتی برای بقا و تاب‌آوری کسب‌وکارها و سازمان‌ها محسوب می‌شود.

این راهنما با تمرکز ویژه بر شرایط بحران، جنگ و اختلال‌های شدید ناشی از آن، به کسب‌وکارها و سازمان‌ها کمک می‌کند تا بر پایه استانداردهای بین‌المللی، اقدامات لازم برای محافظت از داده‌ها و تداوم فعالیت‌های حیاتی خود را طراحی و اجرا کنند. توصیه‌های ارائه‌شده در این سند، مبتنی بر برخی از استانداردهای معتبر جهانی در زمینه امنیت دیجیتال از جمله موارد زیر است:

۱. استاندارد سیستم مدیریت اطلاعات حریم خصوصی[۱] ISO/IEC 27701
۲. استاندارد سیستم مدیریت تداوم کسب‌وکار[۲] ISO/IEC 22301
۳. استاندارد سیستم مدیریت امنیت اطلاعات[۳] ISO/IEC 27001
٤. استاندارد فناوری اطلاعات - فنون امنیتی - آیین‌کار مدیریت امنیت اطلاعات[۴] ISO/IEC 27002
٥. استاندارد امنیت اطلاعات، امنیت سایبری و حفاظت از حریم خصوصی- راهنمای مدیریت ریسک‌های امنیت اطلاعات[۵] ISO/IEC 27005

این راهنما به‌گونه‌ای طراحی شده که برای سازمان‌ها با اندازه‌ها و حوزه‌های کاری مختلف و به‌ویژه کسب‌وکارهای بخش خصوصی کاربردی باشد. مطالب در پنج بخش تنظیم شده است و مباحثی از جمله «درک و ارزیابی ریسک»، «برنامه‌ریزی امنیتی»، «حفاظت از حریم خصوصی داده‌ها»، «تداوم عملیات در بحران» و «انطباق و بهبود مستمر» را پوشش می‌دهد.

هدف این راهنما، ارائه نقشه راهی عملیاتی در شرایط بحران برای حفظ امنیت دیجیتال کسب‌وکارهاست. البته رویکرد مطلوب این است که استانداردهای نام‌برده شده، در شرایط عادی به طور کامل در کسب‌وکارها پیاده‌سازی شوند. این راهنما، فقط خلاصه‌ای از مهم‌ترین نکات این استانداردها را که قابل اجرا در شرایط بحرانی هستند معرفی می‌کند. بنابراین برای اطلاعات بیشتر می‌توانید به آنها مراجعه کنید.

1- Privacy Information Management System (PIMS)
2- Societal Security – Business Continuity Management Systems (BCMS)
3- Information Security Management System (ISMS)
4- Information Technology – Security Techniques - Code of Practice for Information Security Management
5- Information Security, Cybersecurity and Privacy Protection – Guidance on Managing Information Security Risks

۱- درک و ارزیابی ریسک در شرایط بحران

در شرایط بحران، مانند جنگ یا حملات سایبری گسترده، نخستین گام برای حفظ امنیت و پایداری کسب‌وکار، شناسایی دقیق تهدیدها و ارزیابی ریسک‌های مرتبط است. این مرحله زیربنای اقدامات بعدی در مدیریت امنیت اطلاعات و حریم خصوصی است.

۱-۱- شناخت سازمان کسب‌وکار و بستر آن

۱-۱-۱- تعیین و ارزیابی مداوم عوامل داخلی و خارجی مرتبط

برای اینکه بتوانید در شرایط بحرانی به‌موقع واکنش نشان بدهید، لازم است یک گروه داخلی یا مشاور خارجی مشخص کنید که مسئول رصد و تحلیل منظم گزارش‌ها، بخشنامه‌های دولتی، تصمیمات قضایی جدید و تغییرات قوانین داخلی و بین‌المللی مرتبط با حفاظت از داده‌ها و عملیات تجاری باشد.

این گروه باید به‌طور خاص، وضعیت امنیتی کشور، دستورالعمل‌های دفاع سایبری نهادهای دولتی و الزامات اضطراری مربوط به حفظ داده‌ها را بررسی کند.

۱-۱-۲- گسترش مفهوم «امنیت اطلاعات» به «امنیت اطلاعات و حفظ حریم خصوصی»

در همه سیاست‌ها، رویه‌ها و مستندات سیستم مدیریت امنیت اطلاعات (ISMS)، باید عبارت «امنیت اطلاعات» را با «امنیت اطلاعات و حفظ حریم خصوصی» جایگزین کنید و مطمئن شوید که این تغییر در سطح سازمان اطلاع‌رسانی شده و برای همه قابل درک است.

۱-۱-۳- شناسایی و مستندسازی دقیق نقش‌های مربوط به داده‌های هویت شخصی یا شناسایی‌کننده اشخاص[1]

داده‌های هویت شخصی اطلاعاتی هستند که به تنهایی یا در ترکیب با سایر داده‌ها می‌توانند هویت یک فرد حقیقی را مشخص کنند. به عنوان مثال شماره ملی، شماره تلفن، آدرس ایمیل، IP، شماره کارت بانکی و غیره.

در هر فرآیند پردازش داده‌های شخصی، سازمان‌ها یا نقش «کنترل‌کننده» (به معنای تعیین‌کننده اهداف و ابزار پردازش) و یا نقش «پردازشگر» (به معنای انجام‌دهنده پردازش به نمایندگی از کنترل‌کننده) و یا به طور همزمان، هر دو نقش را دارند.

لازم است در فرآیند پردازش داده‌های شخصی در کسب‌وکارتان مشخص کنید که سازمان شما چه نقشی دارد یعنی کنترل‌کننده است یا پردازش‌گر یا هر دو. به عنوان مثال در یک فروشگاه اینترنتی بزرگ که

1- Personally Identifiable Information (PII)

واحدهای مختلفی دارد، یک واحد به طور ویژه در خصوص جمع‌آوری، نگهداری و بهره‌برداری از داده‌های مشتریان مانند سوابق خرید، علایق یا اطلاعات تماس تصمیم‌گیری می‌کند و بنابراین نقش کنترل‌کننده را دارد و واحد دیگری مسئول پیاده‌سازی سیاست‌های فنی مرتبط با حفاظت از داده‌ها مانند رمزنگاری، پشتیبان‌گیری یا مدیریت دسترسی است و در نتیجه، نقش پردازشگر را ایفا می‌کند. این مثالی از کسب‌وکاری است که همزمان هر دو نقش کنترل‌کننده و پردازشگر را دارد. اگر کسب‌وکار شما هر دو نقش را دارد، باید مسئولیت‌ها و اقدامات مربوط به هر نقش را به‌طور جداگانه تعریف و اجرا کنید.

با این حال، ممکن است کسب‌وکار شما در مقیاس کوچک‌تری فعالیت کند مثلاً یک فروشگاه اینترنتی کوچک که از خدمات ابری یک شرکت دیگر برای نگهداری داده‌های مشتریان استفاده می‌کند. این شما هستید که تصمیم می‌گیرید چه داده‌هایی جمع‌آوری شود، چگونه استفاده شود و برای چه مقاصدی به کار گرفته شود بنابراین، نقش شما کنترل‌کننده و نقش شرکت همکارتان، پردازشگر است.

۲-۱- شناخت نیازها و انتظارات طرف‌های ذی‌نفع

۱-۲-۱- شناسایی فعال طرف‌های ذی‌نفع و تضاد منافع

فهرستی از همه طرف‌های ذی‌نفع مانند افرادی که داده‌های شخصی به آنها مربوط است، مشتریان، نهادهای ناظر، تأمین‌کنندگان و حتی رقبا تهیه کنید. در شرایط جنگی، مهاجمان را نیز به‌عنوان طرف ذی‌نفع اما با منافع متضاد در نظر بگیرید.

اگر شرکت بزرگی هستید لازم است یک گروه داخلی مثل تیم امنیت سایبری داخلی که می‌تواند زیرمجموعه یا متشکل از واحد فناوری اطلاعات باشد، باید به‌طور فعال فعالیت‌های مهاجمان یعنی گروه‌های سایبری دولت متخاصم، تروریست‌ها یا مزدوران سایبری را زیر نظر داشته باشد. اگر جزو شرکت‌های کوچک یا متوسط هستید یا به هر دلیلی نمی‌توانید چنین گروه داخلی را داشته باشید، لازم است در این زمینه از خدمات پیمانکاران یا مشاوران متخصص خارج از شرکت استفاده کنید. شناسایی شرکت‌های فعال در این زمینه و انعقاد قرارداد با پیمانکاران، امنیت شرکت را تقویت می‌کند. یکی از فعالیت‌های این تیم چه داخلی باشد چه پیمانکار خارجی، تحلیل اهداف این مهاجمان است تا کنترل‌های امنیتی را به‌شکلی طراحی کند که توانایی خنثی‌سازی تلاش‌های آنها را داشته باشد.

۳-۱- ارزیابی ریسک امنیت اطلاعات و حریم خصوصی

۱-۳-۱- تعریف و بازبینی مداوم معیارهای پذیرش ریسک

مدیر ارشد باید مشخص کند که در شرایط مختلف، از جمله بحران‌های جنگی، چه سطحی از ریسک برای سازمان قابل‌قبول است. این معیارها شامل آستانه‌های مشخص برای خسارت مالی، تأثیر بر عملیات و نقض حریم خصوصی می‌شود و باید به‌صورت منظم بازبینی و تأیید شوند.

۲-۳-۱- شناسایی جامع ریسک‌ها با تمرکز بر سناریوهای جنگی

با استفاده از رویکرد سناریومحور، باید سناریوهای واقعی و محتمل از حملات سایبری و فیزیکی در شرایط جنگ شناسایی و مستندسازی شوند. در ادامه، سه سناریو به عنوان سناریوهای فرضی معرفی می‌شوند.

حملات سایبری

- حمله DDoS[1] به زیرساخت‌های حیاتی
- انتشار بدافزارهای تخریب‌گر یا باج‌افزار
- جاسوسی سایبری با هدف سرقت اطلاعات حساس
- دستکاری داده‌ها برای ایجاد اختلال در زنجیره تأمین یا عملیات مالی

تهدیدهای فیزیکی ناشی از جنگ

- آسیب به تأسیسات حیاتی (مانند مراکز داده یا دفاتر اصلی)
- قطعی گسترده و طولانی‌مدت برق یا شبکه

تهدیدهای انسانی

- خرابکاری توسط کارکنان ناراضی یا نفوذی
- اشتباه انسانی به‌دلیل استرس و خستگی کارکنان

۳-۳-۱- شناسایی و تحلیل منابع ریسک در شرایط جنگی

در این مرحله باید برای هر سناریو، منبع ریسک را مشخص کنید. برخی از منابع ریسک شامل موارد زیر است:

ریسک انسانی (عمدی و غیرعمدی)

- عمدی: کشورهای متخاصم، گروه‌های تروریستی یا مزدور سایبری، هکتیویست‌ها[2]
- غیرعمدی: اشتباه کارکنان

ریسک محیطی

ریسک محیطی مواردی همچون بلایای طبیعی یا خرابی زیرساخت‌ها در اثر حملات جنگی را در بر می‌گیرد.

۱- Distributed Denial of Service: حمله‌ای سایبری که با ارسال حجم زیادی از درخواست‌های جعلی، سیستم هدف را از کار می‌اندازد.

۲- هکتیویست (ترکیب Hacker و Activist) به هکرهایی گفته می‌شود که برای اهداف سیاسی یا اجتماعی سیستم‌ها را هک می‌کنند.

ریسک فنی

ریسک فنی به نقص سیستم‌ها یا خرابی سخت‌افزارها اشاره دارد.

۴-۳-۱- تحلیل ریسک‌ها با ارزیابی پیامدها و احتمال وقوع

برای هر ریسک باید ارزیابی دقیقی از پیامدها انجام بدهید که شامل موارد زیر است:

- مالی (ضررها و جرایم)
- عملیاتی (اختلال خدمات یا زنجیره تأمین)
- شهرت (اعتماد مشتریان و آسیب به شهرت برند به دلیل نقض امنیت سایبری)
- قانونی (نقض مقررات به دلیل از بین رفتن امنیت سایبری و شکایت‌های احتمالی)

تأثیر ریسک‌ها بر حریم خصوصی افراد مرتبط با داده‌های شخصی به آنها مربوط است هم باید به‌طور خاص در نظر گرفته شود.

علاوه بر این، احتمال وقوع هر سناریو را با توجه به انگیزه و توان مهاجم، آسیب‌پذیری‌های موجود و اثربخشی کنترل‌های فعلی ارزیابی کنید. بهتر است این ارزیابی‌ها به‌صورت گروهی انجام شود تا دقت بیشتری داشته باشد.

۵-۳-۱- ارزیابی و اولویت‌بندی ریسک‌ها برای برنامه‌ریزی مقابله

مرحله پایانی این بخش، تحلیل نتایج ریسک با معیارهای پذیرش ریسک است تا مشخص شود کدام ریسک‌ها قابل‌قبول هستند و کدامیک نیاز به اقدام دارند. سپس ریسک‌ها را بر اساس اهمیت که ترکیبی از پیامد و احتمال را در نظر می‌گیرد، اولویت‌بندی کنید تا بتوانید منابع خود را روی مهم‌ترین تهدیدها متمرکز کنید.

۲- برنامه‌ریزی و استراتژی برای تداوم و امنیت

پس از شناسایی ریسک‌ها، گام بعدی طراحی برنامه‌ها و انتخاب راهبردهایی برای مقابله با تهدیدات و حفظ امنیت و تداوم فعالیت‌ها در شرایط بحران است. این مرحله شامل تعیین اهداف امنیتی و اجرای کنترل‌های مؤثر می‌شود.

۲-۱- اهداف امنیت اطلاعات و حفظ حریم خصوصی

۲-۱-۱- تعیین اهداف SMART

برای امنیت اطلاعات و حریم خصوصی، باید اهدافی مشخص[۱]، قابل‌اندازه‌گیری[۲]، دست‌یافتنی[۳]، مرتبط[۴] و دارای زمان‌بندی[۵] تعیین کنید. از سرواژه انگلیسی این ویژگی‌ها کلمه SMART به معنای هوشمند از این ویژگی‌ها تشکیل می‌شود. در اینجا مثال‌هایی از اهداف اسمارت را با هم مرور می‌کنیم.

- حفظ دسترسی‌پذیری خدمات کلیدی آنلاین با ۹۵ درصد آپ‌تایم در طول بحران
- کاهش زمان شناسایی و پاسخ به حوادث امنیتی مربوط به داده‌های هویت شخصی به کمتر از ۲ ساعت

شما می‌توانید متناسب با سازمان و کسب‌وکارتان، اهداف خود را تعیین کنید. این اهداف باید محرمانگی، یکپارچگی، دسترسی‌پذیری اطلاعات و همچنین حفظ حریم خصوصی افراد را دربر بگیرند.

۲-۲- برنامه‌ریزی مقابله با ریسک

۲-۲-۱- انتخاب راهبردهای مقابله با ریسک

برای هر ریسک شناسایی‌شده، لازم است یکی از چهار راهبرد زیر را در نظر بگیرید:

- **اجتناب از ریسک:** به عنوان مثال جمع‌آوری برخی داده‌های حساس را متوقف کنید.
- **کاهش ریسک:** با اجرای کنترل‌ها، احتمال وقوع یا شدت اثر ریسک را کم کنید.
- **پذیرش ریسک:** اگر ریسک کم‌اهمیت یا هزینه کنترل آن زیاد است، آگاهانه آن را بپذیرید.
- **انتقال ریسک:** با اقداماتی شناسایی و عقد قرارداد با پیمانکاران متخصص در زمینه امنیت سایبری، خرید بیمه سایبری[۶] یا قرارداد با ارائه‌دهنده خدمات امن با تعهد سطح بالای خدمات[۷] بالا می‌توانید ریسک خود را منتقل کنید.

1- Specific
2- Measurable
3- Achievable
4- Relevant
5- Time-bound

۶- Cyber Insurance، برخی از شرکت‌های بیمه‌ای در ایران مانند بیمه سامان، بیمه ایران و بیمه سینا، اقدام به ارائه پوشش‌های بیمه‌ای مرتبط با تهدیدهای سایبری کرده‌اند. این پوشش‌ها شامل خسارات مالی ناشی از حملات سایبری، سرقت اطلاعات، اختلال در سیستم‌های اطلاعاتی و برخی آسیب‌های دیگر است. این پوشش‌ها در حال حاضر در سطح محدودی ارائه می‌شوند. (روزنامه دنیای اقتصاد، ۱۴۰۴/۰۱/۲۷، غفلت ایران از بیمه سایبری)

7- Service Level Agreement

۲-۲-۲- تعیین و دسته‌بندی کنترل‌ها

برای هر کنترل امنیتی، لازم است دلیل به‌کارگیری وضعیت اجرایی آن و ارتباطش با نیازهای سازمان مستند شود. سپس کنترل‌ها را در سه گروه زیر دسته‌بندی کنید:

- **پیشگیرانه:** جلوگیری از وقوع مشکل (به عنوان مثال با استفاده از فایروال[۱])
- **شناسایی‌کننده:** تشخیص وقوع مشکل (به عنوان مثال با استفاده از سیستم تشخیص نفوذ[۲])
- **اصلاحی:** کاهش پیامدها بعد از وقوع (به عنوان مثال با پشتیبان‌گیری[۳])

۲-۳- پیاده‌سازی و تقویت کنترل‌های کلیدی در شرایط جنگ

کنترل‌های امنیتی در چهار دسته کلی زیر قرار می‌گیرند:

۲-۳-۱- کنترل‌های سازمانی

- **سیاست‌های امنیتی:** سیاست‌های مدیریت دارایی‌های اطلاعاتی، مدیریت دسترسی و امنیت دیجیتال در بحران خود را بازبینی کنید. اگر چنین سیاستی در سازمان کسب‌وکار شما تعریف نشده است، آن را تدوین کنید. هدف از سیاست امنیت دیجیتال در بحران این است که روش مقابله با تهدیدهای جنگی مشخص شود.
- **مدیریت حوادث:** یک تیم واکنش سریع تشکیل دهید و مراحل شناسایی، طبقه‌بندی، پاسخ‌دهی و گزارش‌دهی به‌ویژه برای نقض داده‌های شخصی را تعریف کنید. این مراحل باید شامل جدول زمان‌بندی برای اطلاع‌رسانی به مراجع قانونی و افراد مربوط نیز باشد.
- **مدیریت تغییرات:** تغییرات را ثبت کنید تا قابل ردیابی باشند و در مواقع بحران، بتوان منشأ اختلال یا آسیب‌پذیری را به‌سرعت شناسایی کرد.
- **سرویس‌های اطلاعات تهدید[۴]:** در سرویس‌های به‌روزرسانی اطلاعات تهدید عضو شوید، یا با نهادهای دولتی و خصوصی همکاری کنید تا هشدارهای امنیتی مرتبط با تهدیدات خاص، به‌ویژه در شرایط جنگ یا بحران، را دریافت کنید. شاید بتوان VirusTotal گوگل را یکی از انواع این سرویس‌ها دانست.

1- Firewall

۲- سیستم تشخیص نفوذ Intrusion Detection System (IDS)

3- Backup

4- Threat Intelligence

۲-۳-۲- کنترل‌های انسانی

- **آموزش و آگاهی‌بخشی:** جلسات آموزش‌های امنیت سایبری را به صورت منظم برگزار کنید. باید در این جلسات، سناریوهایی مانند حملات فیشینگ یا مهندسی اجتماعی[۱] مرتبط با موضوعات جنگی تمرین شود. علاوه بر این، کارکنان درباره پیامدهای قانونی و مالی نقض اطلاعات آگاه شوند.
- **شناسایی افراد کلیدی:** کارکنانی را شناسایی کنید که در شرایط بحرانی، توانایی حفظ آرامش، رعایت دقیق پروتکل‌ها و اتخاذ تصمیم‌های کم‌خطا را دارند. این افراد معمولاً در برابر فشار روانی مقاوم‌تر هستند و در مواقع بحران، خطای انسانی کمتری از آنها – که بنا به شرایط ممکن است اجتناب‌ناپذیر باشد- دیده می‌شود. حضور این افراد در تیم‌های کلیدی مدیریت بحران، واکنش سریع و امنیت اطلاعات به دلیل تسلط بر شرایط توصیه می‌شود.
- **بازبینی قراردادهای محرمانگی:** قراردادها با کارکنان، پیمانکاران و شرکا را با تأکید بر وظایف‌شان در شرایط اضطراری مورد بازبینی قرار دهید.
- **سیاست‌های دورکاری امن:** کارکنان را ملزم به استفاده از VPN کنید. احراز هویت چندعاملی را فعال کنید و دسترسی به دستگاه‌های شخصی مانند موبایل یا لپ‌تاپ کارکنان را کنترل کنید.

۲-۳-۳- کنترل‌های فیزیکی

- **حفاظت فیزیکی:** امنیت ساختمان‌ها را با موانع فیزیکی بیشتر، افزایش نیروهای حفاظتی و سخت‌گیری در ورود و خروج تقویت کنید.
- **مقابله با تهدیدهای محیطی:** اقدامات محافظتی در برابر آتش‌سوزی، سیل و آسیب‌های ناشی از جنگ را پیش‌بینی و لحاظ کنید.
- **دفع امن تجهیزات:** برای حذف یا نابودسازی مطمئن تجهیزات ذخیره‌سازی حاوی داده‌های حساس مثلا انواع هارد، فلش و موبایل آمادگی داشته باشید.

۲-۳-٤- کنترل‌های فناوری

- **رمزنگاری:** برای همه داده‌های حساس در حال ذخیره یا انتقال و نیز مدیریت کلیدها[۲]به‌صورت متمرکز و امن رمزگذاری قوی انجام دهید.
- **مدیریت دسترسی:** اصل حداقل دسترسی[۳] را اجرا کنید و دسترسی‌های بلااستفاده را به‌صورت دوره‌ای حذف یا اصلاح کنید.

۱- Phishing & Social Engineering Attack، حملات فیشینگ و مهندسی اجتماعی با فریب کاربران از طریق ایمیل، پیامک یا تماس تلفنی، اطلاعات حساس مانند رمز عبور یا کد تأیید آنها را دریافت می‌کنند.

۲- Key Management به نگهداری، توزیع و محافظت از کلیدهای رمزنگاری برای حفظ محرمانگی داده‌ها گفته می‌شود.

۳- Least Privilege یعنی هر فرد فقط به آنچه نیاز دارد دسترسی داشته باشد، نه بیشتر.

- **ظرفیت و افزونگی**[1]: این مورد به توانایی سیستم برای مدیریت بار کاری و حفظ تداوم عملیات با استفاده از منابع اضافی در صورت خرابی اشاره دارد. لازم است ظرفیت سیستم‌ها را به‌صورت مداوم بررسی کنید و آنها را در شرایط بحران برای اهدافی مانند مقابله با DDoS آنها توسعه دهید. همچنین زیرساخت‌های جایگزینی را برای تضمین دسترسی حتی در صورت از کار افتادن بخشی از سیستم، پیاده‌سازی کنید.
- **محافظت در برابر بدافزار**: ابزارهای ضد بدافزار و سیستم‌های تشخیص/پاسخ نقطه پایانی[2] را نصب، به‌روزرسانی و بر آنها نظارت کنید.
- **محافظت از نقاط پایانی[3] در برابر تهدیدها**: برای حفاظت از دستگاه‌هایی مثل رایانه‌ها، لپ‌تاپ‌ها و موبایل‌هایی که به شبکه متصل می‌شوند، از ابزارهای امنیتی مانند آنتی‌ویروس‌های پیشرفته و سیستم‌های EDR استفاده کنید.
- **پشتیبان‌گیری**: استراتژی «۳-۲-۱» را در پشتیبان‌گیری اجرا کنید. این استراتژی می‌گوید ۳ نسخه پشتیبان، روی ۲ نوع رسانه و ۱ نسخه پشیبان آفلاین/خارج از سایت تهیه کنید. نحوه بازیابی اطلاعات را تمرین کنید و مانور بازیابی اطلاعات برگزار کنید. نسخه‌های پشتیبان را به صورت جغرافیایی و ترجیحاً خارج از منطقه درگیری، پراکنده کنید یا به اصطلاح همه تخم مرغ‌هایتان را در یک سبد نچینید و نسخه‌های پشتیبان را در یک مکان متمرکز نگه ندارید.
- **ثبت و پایش**: رویدادهای سیستمی را به‌صورت متمرکز ثبت کنید. همچنین لازم است این اطلاعات به‌صورت مداوم برای تشخیص رفتارهای غیرعادی، پایش شوند. علاوه بر این لاگ‌ها[4]را حفظ کنید چرا که ممکن است برای تحلیل‌های قضایی در آینده مورد استفاده قرار بگیرند.
- **امنیت شبکه**: شبکه را برای حفاظت از سیستم‌های حیاتی، استفاده از فایروال‌های پیشرفته و سیستم‌های تشخیص و پیشگیری[5] نفوذ را جداسازی کنید.
- **امنیت در توسعه**: در چرخه توسعه نرم‌افزار اصل «حریم خصوصی بر اساس طراحی»[6] را اجرا کنید. یعنی حریم خصوصی افراد را از همان مراحل اولیه طراحی سیستم‌ها، فرایندها و نرم‌افزارها در نظر بگیرید نه اینکه بعداً به آن اضافه کنید. همچنین دقت داشته باشید محیط‌های توسعه، تست و تولید نرم‌افزارها را جداسازی کنید.

1- Capacity and Redundancy

۲- Endpoint Detection and Response (EDR): ابزارهایی که رفتار دستگاه‌ها مثلاً لپ‌تاپ کارکنان را بررسی می‌کنند و می‌توانند به تهدیدها واکنش سریع داشته باشند.

۳- Endpoints یا نقاط پایانی به دستگاه‌هایی مانند رایانه، لپ‌تاپ یا تلفن همراه گفته می‌شود که با اتصال به شبکه امکان تبادل داده را دارند.

۴- Logs: گزارش رویدادهای سیستم که می‌تواند شامل مواردی همچون چه کسی، چگونه و از کجا به سیستم وارده شده است، باشد.

۵- سامانه‌های تشخیص نفوذ Intrusion Detection System (IDS) و پیشگیری از نفوذ Intrusion Prevention System (IPS) ابزارهایی هستند که با رصد ترافیک شبکه، تهدیدهای احتمالی را شناسایی می‌کنند. IDS هشدار می‌دهد و IPS به‌طور خودکار جلوی تهدید را می‌گیرد.

6- Privacy by Design

- **داده‌های آزمایشی:** داده‌های واقعی افراد در فرآیندهای آزمایش استفاده نکنید. اگر ناچار به استفاده از داده‌های ناشناس هستید، آنها را ناشناس‌سازی[1] یا جایگزین[2] کنید و همان سطح امنیت محیط تولید را رعایت کنید. ناشناس‌سازی به معنای حذف همه اطلاعات شناسایی‌کننده بدون امکان بازگشت است. جایگزین کردن نیز به جایگزینی اطلاعات شناسایی‌کننده با رمز یا کد اشاره دارد که در صورت وجود کلید برای بازگشایی این رمزها، قابل بازگشت است.

۳- حفظ حریم خصوصی داده‌ها

در شرایط بحرانی، حفاظت از داده‌های شخصی اهمیت ویژه‌ای پیدا می‌کند. اجرای چارچوب مدیریت اطلاعات شناسایی‌کننده شخصی[3] به کسب‌وکار شما کمک می‌کند از حقوق افراد مرتبط با داده‌ها حفاظت و از ریسک‌های قانونی و آسیب به شهرت جلوگیری کنید.

چارچوب مدیریت داده‌های شناسایی‌کننده شخصی مجموعه‌ای از سیاست‌ها، فرایندها و کنترل‌های سازمان‌یافته است که با هدف حفاظت از داده‌های شناسایی‌کننده شخصی (PII) و اطمینان از رعایت اصول حریم خصوصی افراد، در یک سازمان پیاده‌سازی می‌شود.

۳-۱- شرایط جمع‌آوری و پردازش PII

۳-۱-۱- مستندسازی هدف و مبنای قانونی

برای هر نوع داده شخصی که جمع‌آوری یا پردازش می‌کنید، باید هدف مشخص و مبنای قانونی آن را مانند رضایت صریح، الزامات قراردادی، تعهدات قانونی یا منافع مشروع، به‌طور شفاف مستند کنید. ممکن است در صورت نیاز این اسناد را در اختیار نهادهای ناظر قرار دهید.

۳-۱-۲- مدیریت رضایت افرادی که داده‌های شخصی به آنها مربوط است

لازم است فرآیندی استاندارد برای گرفتن، ثبت، به‌روزرسانی یا لغو رضایت افراد مرتبط با داده‌های شخصی پیاده‌سازی کنید. مهم است که لغو رضایت به همان سادگی گرفتن رضایت باشد. برای مثال اگر رضایت افراد را در یک فرم یا یک تیک به صورت آنلاین دریافت می‌کنید، امکان لغو آنلاین را هم فراهم کنید.

مثال‌هایی از این نوع رضایت افراد، در تکمیل انواع پرسشنامه‌های آنلاین است. مثلاً اگر یک فروشگاه اینترنتی، هنگام ثبت نام کاربر، گزینه جداگانه‌ای با متن «با جمع‌آوری و ذخیره اطلاعات جست‌وجوهای من

1- Anonymization
2- Pseudonymization
3- PIMS – Privacy Information Management System

برای ارائه خدمات بهتر موافق هستم»نمایش بدهد و کاربر به انتخاب خود آن را انتخاب کند، دریافت رضایت رخ داده است و لغو آن نیز باید به سادگی در صفحه کاربر قابل دسترسی باشد.

۳-۱-۳- ارزیابی تأثیر بر حریم خصوصی[1]

پیش از اجرای هر پروژه جدید یا تغییر مهم در فرآیندهای موجود که شامل پردازش داده‌های شخصی است، باید تأثیر آن را بر حریم خصوصی ارزیابی کنید. این ارزیابی به شناسایی و کاهش ریسک‌های مرتبط با حریم خصوصی کمک می‌کند.

۳-۱-٤- قراردادهای سخت‌گیرانه با پردازشگران داده

قراردادهایی که با پیمانکاران یا پردازشگرهای داده امضا می‌کنید باید شامل بندهای الزام‌آور و دقیق درباره امنیت و حفظ حریم خصوصی باشد. این قراردادها، توافق‌نامه‌هایی هستند که بین سازمان (کنترل‌کننده داده) و پیمانکاران یا شرکت‌هایی که داده‌ها را پردازش می‌کنند (پردازشگران داده) امضا می‌شوند.

هدف اصلی این قراردادها تضمین این است که پردازشگر داده‌ها، الزامات امنیتی و حریم خصوصی را به‌طور دقیق و کامل رعایت کند. شما می‌توانید این الزامات را بر اساس پیوست B استاندارد ISO/IEC 27701 تنظیم کنید.

۳-۱-٥- مستندسازی سوابق پردازش داده‌های هویتی شخصی

یک فهرست موجودی پردازش برای داده‌های شناسایی‌کننده اشخاص ایجاد کنید که شامل نوع داده، هدف، گروه‌های مرتبط و اقدامات امنیتی مربوط به آن باشد. این فهرست باید همیشه به‌روز شود و آماده ارائه به نهادهای ناظر باشد.

۳-۲- تعهدات در قبال افرادی که داده‌های شخصی به آنها مربوط است

۳-۲-۱- احترام به حقوق افراد

سازوکارهایی ساده، قابل‌دسترسی و شفاف ایجاد کنید تا افراد بتوانند حقوق خود را اجرا کنند: مثلاً دسترسی به داده‌ها، اصلاح یا حذف آنها، اعتراض به پردازش یا درخواست انتقال. لازم است یک نقطه تماس مشخص برای رسیدگی به این درخواست‌ها تعیین شود، که با شیوه جمع‌آوری داده‌ها هماهنگ باشد.

۳-۲-۲- اطلاع‌رسانی به دریافت‌کنندگان ثالث در صورت تغییر

اگر داده‌های فردی به درخواست شخص تغییر یا حذف شود، باید فرآیندی وجود داشته باشد که این تغییرات را به تمام دریافت‌کنندگان ثالث نیز اطلاع بدهد. حفظ ارتباط مؤثر با این طرف‌ها ضروری است.

1- Privacy Impact Assessment

۳-۳- حریم خصوصی بر اساس طراحی و پیش‌فرض

۳-۳-۱- حداقل‌سازی داده و تنظیمات پیش‌فرض ایمن

در طراحی سیستم‌ها و فرآیندها، باید تضمین شود که فقط مقدار حداقلی از داده‌های شخصی موردنیاز جمع‌آوری و پردازش شود. همچنین تنظیمات پیش‌فرض هر سیستم باید در راستای حفظ حریم خصوصی باشد.

۳-۳-۲- تضمین دقت و کیفیت داده‌های شخصی

باید سازوکاری وجود داشته باشد که از صحت، کامل بودن و به‌روز بودن داده‌های شخصی در تمام مدت نگهداری آنها اطمینان حاصل شود. علاوه بر این، باید روندی برای اصلاح خطاها یا رسیدگی به درخواست‌های اصلاحی افراد تعریف شده باشد.

۳-۳-۳- صرفه‌جویی در داده

اهداف مشخصی برای کاهش جمع‌آوری و نگهداری داده تعیین کنید. مثلاً در مواقعی که نیازی به اطلاعات کامل نیست، از تکنیک‌هایی مانند نام‌مستعارسازی یا ناشناس‌سازی استفاده کنید.

۳-۳-٤- مدیریت نگهداری و حذف امن داده‌ها

برای نگهداری داده‌های شخصی، جدول زمانی مشخصی بر اساس الزامات قانونی، نظارتی و تجاری تهیه کنید. همچنین، باید فرآیند مستندی برای حذف ایمن داده‌ها، از جمله فایل‌های موقت وجود داشته باشد. این فرآیند باید تضمین کند که داده‌ها به‌صورت غیرقابل بازیابی حذف شوند؛ به‌ویژه در شرایط بحرانی که خطر افتادن اطلاعات به دست دشمن وجود دارد.

۳-۳-۵- امنیت در انتقال داده‌ها

هنگام ارسال داده‌های شخصی از طریق شبکه، باید از روش‌هایی مانند رمزنگاری، کنترل دسترسی و ثبت وقایع استفاده شود تا امنیت انتقال تضمین شود و داده‌ها فقط به مقصد موردنظر برسد.

۳-٤- اشتراک‌گذاری، انتقال و افشای PII

۳-٤-۱- مستندسازی مبنای انتقال بین‌المللی

اگر قصد دارید داده‌های شخصی را به خارج از کشور یا به سیستم‌های حقوقی دیگر منتقل کنید، باید مبنای قانونی این انتقال را مشخص و مستند کنید. کسب‌وکارها باید مشخص کنند که داده‌ها به کدام کشورها یا سازمان‌های بین‌المللی ارسال می‌شود و این اطلاعات را به مشتریان اطلاع دهند.

۳-٤-۲- ثبت سوابق همه انتقال‌ها و افشاها

برای همه موارد انتقال یا افشای داده‌های شخصی، یک دفتر ثبت دقیق نگهداری کنید که شامل این اطلاعات باشد: **چه داده‌ای، به چه کسی، در چه زمانی** و **با چه مجوزی** منتقل شده است. درخواست‌های قانونی مراجع قضایی یا امنیتی هم مشمول ثبت در دفتر هستند.

۳-٤-۳- شفافیت در استفاده از پیمانکاران فرعی

باید مشتریان خود را قبل از اینکه پیمانکاران فرعی در پردازش داده‌های شخصی شروع به کار کنند، از این موضوع مطلع کنید. اطمینان حاصل کنید که قرارداد با این پیمانکاران، آنها را ملزم به رعایت الزامات امنیتی و حریم خصوصی، حتی سخت‌گیرانه‌تر از استانداردهای داخلی شما، کند.

٤- عملیات و تداوم کسب‌وکار در بحران

در میانه بحران، حفظ تداوم فعالیت‌های کلیدی کسب‌وکار شما حیاتی است. به همین دلیل با برنامه‌ریزی عملیاتی و ایجاد ساختارهای واکنش سریع می‌توانید توقف عملیات کاری را کاهش و آمادگی سازمان در برابر اختلال‌ها را افزایش دهید.

٤-۱- برنامه‌ریزی و کنترل عملیاتی

٤-۱-۱- تعریف و کنترل فرایندهای حیاتی

باید برای همه فرایندهای عملیاتی، به‌ویژه آنهایی که با داده‌های شناسایی‌کننده اشخاص سروکار دارند، معیارهای عملکرد و کنترل را مشخص کنید. مستندسازی دقیق این فرایندها و ثبت تغییرات اعم از برنامه‌ریزی‌شده و ناخواسته کمک می‌کند عملیات کسب‌وکارتان به‌درستی و با کمترین اختلال انجام شود.

٤-۱-۲- مدیریت دقیق برون‌سپاری‌ها

در شرایط بحران، باید بر فرایندهای برون‌سپاری‌شده‌ای که به امنیت اطلاعات و داده‌های شخصی مربوط هستند، نظارت سخت‌گیرانه‌تری اعمال کنید. این نظارت‌ها شامل بازبینی مداوم عملکرد تأمین‌کنندگان و ارزیابی ریسک‌های ناشی از وابستگی به آنها است.

٤-٢- سیستم مدیریت تداوم کسب‌وکار[1]

٤-٢-١- توسعه BCMS متناسب با شرایط جنگ

هدف اصلی سیستم مدیریت تداوم کسب‌وکار محافظت از کسب‌وکار در برابر حوادث مخرب، کاهش احتمال وقوع آنها، آمادگی برای واکنش و بازیابی از آنهاست. در این چارچوب، باید «جنگ» صراحتاً به‌عنوان یک سناریوی کلیدی در نظر بگیرید.

٤-٢-٢- ایجاد ساختار واکنش سریع و ارتباطات اضطراری

- **ساختار واکنش:** یک تیم مدیریت بحران با مسئولیت‌ها و نقش‌های مشخص (مانند مسئول فنی، مسئول ارتباطات و مسئول حقوقی) تشکیل دهید. آستانه‌هایی برای فعال‌سازی برنامه‌های BCMS، مانند وقوع حمله سایبری، هشدارهای امنیتی دولتی یا تخریب فیزیکی زیرساخت‌ها، تعریف کنید.
- **ارتباطات اضطراری:** فرآیندهایی برای شناسایی فوری حادثه، پایش مداوم آن و مدیریت ارتباطات داخلی و خارجی تدوین کنید. این موارد شامل استفاده از مسیرهای ارتباطی جایگزین (برای شرایطی که شبکه اصلی قطع است)، دریافت هشدارهای رسمی از نهادهای ملی یا منطقه‌ای و مدیریت ارتباط با رسانه‌ها می‌شود.

٤-٢-٣- برنامه‌های تداوم با جزئیات عملیاتی

باید برای سناریوهای خاص مرتبط با جنگ، مانند از دست رفتن ساختمان و دفتر کار، قطعی اینترنت یا عدم دسترسی به پرسنل، برنامه‌های مشخصی تدوین کنید که هر برنامه باید شامل موارد زیر باشد:

- اهداف بازیابی زمان (RTO[2]) و بازیابی داده (RPO[3]) یعنی حداکثر زمانی که می‌توان سیستم را بعد از بحران غیرفعال نگه داشت و میزان داده‌ای که می‌توان در صورت بحران از دست داد.
- برنامه ارتباط با رسانه‌ها، شامل بیانیه‌های آماده و تعیین سخنگویان رسمی کسب‌وکار شما

٤-٢-٤- رویه‌های بازیابی و بازگشت به وضعیت عادی

پس از پایان بحران، باید گام‌های روشنی برای بازگرداندن عملیات به حالت عادی داشته باشید. این گام‌ها شامل بازیابی سیستم‌ها و داده‌ها از نسخه‌های پشتیبان، اطمینان از صحت و یکپارچگی اطلاعات و راه‌اندازی مجدد فرایندهای حیاتی هستند.

1- Business Continuity Management System (BCMS)
2- Recovery Time Objective
3- Recovery Point Objective

٤-٢-٥- تمرین و به‌روزرسانی منظم برنامه‌ها

برنامه‌های تداوم کسب‌وکار را به‌طور منظم از طریق تمرین‌های واقع‌بینانه مثلاً به‌صورت فصلی یا سالانه آزمایش کنید. این تمرین‌ها باید همه ذی‌نفعان اصلی کسب‌وکار شما را از جمله کارکنان، تأمین‌کنندگان و حتی مشتریان کلیدی را درگیر کند. پس از هر تمرین، باید گزارش‌هایی برای مستندسازی تجربیات و بهبود طرح‌ها تهیه کنید.

٥- انطباق و بهبود مستمر

کسب‌وکار شما باید فرایندی مداوم برای شناسایی، ارزیابی و به‌روزرسانی الزامات قانونی، نظارتی و قراردادی مربوط به امنیت اطلاعات و حریم خصوصی داشته باشد. برای این منظور لازم است الزامات قانونی و قراردادی به صورت مستمر رصد و در صورت نیاز به‌روز شوند.

٥-١- الزامات قانونی و قراردادی

٥-١-١- رصد و به‌روزرسانی فعال الزامات

فرایند رصد و به‌روزرسانی به‌ویژه در شرایط بحرانی مانند وضعیت اضطراری یا تغییر مقررات در زمان جنگ باید فعال‌تر و دقیق‌تر شود. همچنین باید پیامدهای احتمالی عدم انطباق، مانند جریمه‌های مالی، آسیب به شهرت سازمان یا محرومیت از فعالیت در برخی بازارها را به‌درستی شناسایی کنید و در ارزیابی ریسک‌های کلی کسب‌وکارتان در نظر بگیرید.

٥-٢- بازبینی مستقل و حسابرسی داخلی

٥-٢-١- بازبینی مستقل

در بازه‌های زمانی مشخص یا در صورت تغییرات مهم، لازم است بازبینی‌هایی مستقل از مدیریت امنیت اطلاعات و اجرای سیاست‌ها را انجام دهید. این بازبینی‌ها می‌توانند توسط کارشناسان داخلی غیروابسته یا نهادهای ثالث انجام شوند تا دیدگاهی بی‌طرف و دقیق از وضعیت کنونی کسب وکار شما ارائه دهند.

٥-٢-٢- حسابرسی داخلی

لازم است برای سیستم‌های مدیریتی خود از جمله مدیریت امنیت اطلاعات،[1] مدیریت حریم خصوصی اطلاعات[2] و مدیریت تداوم کسب‌وکار[3]، برنامه‌ای مستند برای حسابرسی داخلی داشته باشید. تمرکز این

1- Information Security Management System (ISMS)
2- Privacy Information Management System (PIMS)
3- Business Continuity Management System (BCMS)

حسابرسی‌ها باید بر کنترل‌های مهم، به‌ویژه آنهایی باشد که به سناریوهای بحرانی مانند جنگ مرتبط هستند. نتایج این حسابرسی‌ها را به مدیران ارشد گزارش دهید تا بر اساس آنها تصمیم‌گیری مؤثر انجام شود.

۵-۳- بهبود مستمر

۵-۳-۱- بازنگری مداوم سیستم‌های مدیریتی

برای حفظ کارایی و اثربخشی، باید سیستم‌های مدیریتی مانند ISMS، PIMS و BCMS را به‌طور منظم از نظر تناسب، کفایت و عملکرد بازنگری کنید. این بازنگری‌ها می‌توانند از طریق جلسات مدیریتی، بررسی شاخص‌های عملکرد یا تحلیل حوادث انجام شوند.

۵-۳-۲- تحلیل درس‌آموخته‌ها

پس از هر حادثه امنیتی یا حتی موقعیت‌هایی که به‌طور بالقوه می‌توانستند حادثه‌ساز شوند که به آنها Near Miss[1] گفته می‌شود، باید تحلیلی جامع از درس‌آموخته‌ها انجام دهید. نتایج این تحلیل‌ها برای تقویت کنترل‌ها، اصلاح رویه‌ها و بهبود پاسخ به حوادث مشابه در آینده برای کسب‌وکار شما قابل استفاده هستند.

۵-۳-۳- پایش فعال عوامل مؤثر بر ریسک‌ها

سیستمی برای پایش مداوم عواملی مانند ارزش دارایی‌ها، تهدیدهای جدید، آسیب‌پذیری‌های شناسایی‌شده و تغییرات در احتمال وقوع آنها پیاده‌سازی کنید. این پایش کمک می‌کند تهدیدات احتمالی را زودتر شناسایی کنید و اقدامات مقابله‌ای را با سرعت و اثربخشی بیشتری اجرا کنید.

۵-۴- عدم انطباق و اقدامات اصلاحی

۵-۴-۱- واکنش سریع به عدم انطباق‌ها

در صورت بروز هرگونه عدم انطباق، مانند ضعف در یک کنترل امنیتی یا تخطی از یک سیاست، باید بلافاصله اقدامات کنترلی و اصلاحی را انجام دهید تا اثرات آن کاهش یابد.

۵-۴-۲- تحلیل ریشه‌ای[2] و اصلاح مؤثر

برای هر مورد عدم انطباق، باید علل اصلی آن را شناسایی کنید و اقداماتی مؤثر برای جلوگیری از تکرار آن را در آینده طراحی و اجرا کنید. همچنین ضروری است اثربخشی این اقدامات اصلاحی را به‌طور منظم ارزیابی کنید و در صورت لزوم آنها را بازنگری کنید.

۱- رخدادی که می‌توانست منجر به آسیب، خسارت یا نقض امنیت شود، اما به هر دلیلی اتفاق نیافتاده است.

2- Root Cause Analysis

منابع

1. ISO/IEC 27701: Privacy Information Management System (PIMS)
2. ISO/IEC 22301: Societal Security – Business Continuity Management Systems (BCMS)
3. ISO/IEC 27001: Information Security Management System (ISMS)
4. ISO/IEC 27002: Information Technology – Security Techniques – Code of Practice for Information Security Controls
5. ISO/IEC 27005: Information Security, Cybersecurity and Privacy Protection – Guidance on Managing Information Security Risks