جمهوری اسلامی ایران
ریاست جمهوری

مرکز مدیریت راهبردی افتا

شماره: ۰۰/۸۵۸۷/الف/ع
تاریخ: ۱۴۰۰/۰۷/۲۸
پیوست: دارد

کلیه دستگاه‌های اجرایی کشور (دارای زیرساخت حیاتی)

موضوع: الزامات و اقدامات امنیتی جهت پیشگیری و پاسخ به حوادث سایبری

سلام علیکم

با احترام، با توجه به ضرورت اتخاذ تدابیر لازم برای مقابله با تحریم‌ها و تهدیدات سایبری و تحقق نظام ملی پیشگیری و مقابله با حوادث فضای مجازی و همچنین پیرو مکاتبات قبلی در خصوص موضوع فوق، به پیوست مستند مربوط به "الزامات و اقدامات امنیتی جهت پیشگیری و پاسخ به حوادث سایبری" برای بهره‌برداری ارسال می گردد. لذا خواهشمند است دستور فرمائید ضمن انجام اقدامات پیشگیرانه و حصول اطمینان از اجرای الزامات ابلاغی این مرکز، مستند فوق به کلیه واحدهای تابعه با قید فوریت برای پیاده‌سازی ابلاغ گردد.

جواد درگاهی
رئیس مرکز

دبیرخانه وزارت کشور
تاریخ :۱۴۰۰/۰۷/۲۸
شماره ثبت :۱۱۸۳۱۸

رونوشت:

- جناب آقای دکتر فیروزآبادی دبیر محترم شورای عالی و رئیس مرکز ملی فضای مجازی برای استحضار
- رئیس محترم سازمان حراست کل کشور برای استحضار

آدرس: تهران-خیابان شهید بهشتی-خیابان قائم مقام فراهانی-کوچه شهدا-پلاک ۱ و ۳- تلفن: ۴۳۴۳۹۰۰۰ فاکس: ۸۸۷۱۳۲۳۵ صندوق پستی: ۷۱۷۸-۱۵۸۷۵

جمهوری اسلامی ایران
ریاست جمهوری
مرکز مدیریت راهبردی افتا

الزامات و اقدامات امنیتی جهت پیشگیری و پاسخ به حوادث سایبری

مهر ۱۴۰۰

فهرست

۱) مقدمه

با توجه به حساسیت دستگاه‌های زیرساختی و تأثیرات گسترده و با سرعت بالای آن بر جامعه و با توجه به شرایط خاص کشور در برهه زمانی فعلی و رویکرد همیشگی دشمنان در خصوص انجام حملات سایبری بر علیه این زیرساخت‌ها، مرکز مدیریت راهبردی افتا در راستای افزایش میزان آمادگی دستگاه‌های مربوطه در این بخش‌ها در مقابل این حملات و افزایش پاسخ‌دهی مؤثرتر به این حوادث محتمل، اقدام به تهیه این مستند نموده است. متولیان امنیت فناوری اطلاعات سازمان موظف به رعایت دقیق و کامل این الزامات در شبکه‌های فناوری اطلاعات و صنعتی خود می‌باشند. همچنین لازم است گزارش وضعیت اجرای این الزامات در سازمان را به مرکز مدیریت راهبردی افتا ارسال نمایند. در این سند الزامات امنیتی عملیاتی پایه، در دسته‌های ذیل آورده شده است:

- اقدامات پیشگیرانه
- اقدامات زمان بحران
- اقدامات مدیریتی

۲) اقدامات پیشگیرانه

این دسته از اقدامات به‌منظور پیشگیری از بروز حوادث سایبری در سطح دستگاه‌های زیرساختی انجام شود. این اقدامات در ۸ دسته طبقه‌بندی می‌شوند که عبارتند از:

۲–۱) شناسایی و اشراف بر دارایی‌های اطلاعاتی

- ✓ تمامی سرویس‌ها و سامانه‌های حیاتی سازمان به همراه مؤلفه‌های سخت‌افزاری و نرم‌افزاری، شناسایی و اولویت‌بندی شوند.
- ✓ مستندات کامل و بروز از نیازمندی‌ها و معماری سامانه‌های حیاتی سازمان و همچنین توپولوژی منطقی و فیزیکی شبکه‌های ارتباطی مورداستفاده در آن‌ها تهیه گردد.
- ✓ لیست بروز از پروتکل‌ها و سامانه‌های سخت‌افزاری و نرم‌افزاری مجاز به استفاده در سازمان شناسایی و تدوین گردد.
- ✓ مراکز حساس سازمان (شامل مرکز داده، محل قرارگیری تجهیزات حساس و...) مرتبط با سامانه‌های حیاتی شناسایی شوند.
- ✓ پیمانکاران و شرکت‌های ارائه‌کننده خدمات و محصولات مرتبط با سامانه‌های حیاتی شناسایی شوند؛ به همراه روش‌های ارتباط با سازمان از جمله ابزارهای دسترسی از را دور و VPNهایی که توسط این شرکت‌ها مورداستفاده قرار می‌گیرد.
- ✓ لیست بروز شده از آدرس IPهای معتبر سازمان بر بستر اینترنت و مشخص نمودن سرویس‌های فعال بر روی آن‌ها تهیه شود. لیست مذکور می‌بایست برای مرکز افتا ارسال گردد.
- ✓ مسئولین و متولیان دارایی‌های اطلاعاتی حساس نظیر سامانه‌ها و سرویس‌های حیاتی، سرورها، تجهیزات امنیتی و... شناسایی شوند. در این لیست باید راه‌های ارتباطی با فرد مذکور در مواقع بحران مشخص شده باشد.

۲–۲) مدیریت آسیب‌پذیری‌ها و مخاطرات سایبری

- ✓ سامانه‌های حیاتی خاص سازمان، باید با همکاری مرکز افتا مورد ارزیابی امنیتی قرار گیرند.
- ✓ کلیه سامانه‌های حیاتی به‌طور منظم توسط شرکت‌های دارای پروانه خدمات از مرکز افتا، مورد پویش آسیب‌پذیری واقع‌شده و موارد شناسایی‌شده رفع گردد.

- ✓ مستندات کامل و بروز از مخاطرات سرویس‌ها و سامانه‌های حیاتی سازمان تهیه و تدوین گردد.
- ✓ پیوست امنیتی و راهکار رفع مخاطرات و تأمین امنیت سایبری سرویس‌ها و سامانه‌های حیاتی سازمان تدوین شود.
- ✓ ارائه هر سرویس در بستر اینترنت منوط به انجام آزمون نفوذ و رفع آسیب‌پذیری‌های احتمالی گردد. همچنین ارائه سرویس حیاتی در بستر اینترنت باید با هماهنگی مرکز افتا صورت پذیرد.

۲–۳) مدیریت دسترسی به منابع سازمان

- ✓ دسترسی فیزیکی افراد غیرمجاز به اماکن حساس مرتبط با سامانه‌های حیاتی محدود گردیده و فهرستی از افراد مجاز برای دسترسی به اماکن حساس تهیه گردد.
- ✓ دسترسی کاربران به سامانه‌های حیاتی و سامانه‌های مرتبط با آن‌ها بر اساس اصل حداقل دسترسی (شامل ایجاد، فعال‌سازی و غیرفعال‌سازی، حذف و تغییر سطح دسترسی) محدود و مدیریت شود.
- ✓ دسترسی مشاوران، پیمانکاران و کارکنان موقت به شبکه و سیستم‌های اطلاعاتی سامانه‌های حیاتی محدود و مدیریت شود.
- ✓ مدیریت دسترسی از راه دور به سامانه‌های حیاتی باید با در نظرگیری محدودیت‌های زمان‌بندی و مکانی و پس از کسب مجوزهای لازم انجام شده و دسترسی از خارج کشور به این سامانه‌ها مسدود شود.
- ✓ کلمات عبور انتخابی از پیچیدگی و طول مناسب برخوردار بوده و در بازه‌های زمانی مناسب کاربران مجبور به تغییر آن‌ها شوند و سازوکار مناسبی برای نگهداری آن‌ها در نظر گرفته شود.
- ✓ احراز هویت چندعامله با قابلیت عدم‌انکار در تمامی سرویس‌ها و سامانه‌های حیاتی به‌منظور تصدیق هویت کلیه کاربران فعال شود.
- ✓ از دسترسی غیرمجاز و دست‌کاری لاگ‌های ذخیره‌شده و نسخه‌های پشتیبان جلوگیری شود و نسخه‌های پشتیبان سامانه‌ها و سرویس‌های حیاتی در محیط ایزوله نگهداری شود.
- ✓ دسترسی IPهای خارجی به سرویس‌ها و سامانه‌هایی که برای سرویس‌گیرندگان داخلی هستند محدود شوند.
- ✓ تمامی حساب‌های کاربری مرتبط با سامانه‌های حیاتی شناسایی‌شده و حساب‌های کاربری غیرضروری حذف شوند.
- ✓ فهرست IPهای آلوده شناسایی‌شده و ارتباط سامانه‌های حیاتی سازمان با آن‌ها مسدود شود.

۲–۴) پیکربندی تجهیزات و سامانه‌ها

- ✓ پیکربندی تمامی دارایی‌های مرتبط با سامانه‌های حیاتی (نظیر سوئیچ، روتر، تجهیزات امنیتی، سیستم‌عامل، پایگاه داده، سرویس‌دهنده وب و...) بازبینی‌شده و مطابق با آخرین راهنماهای امنیتی مربوطه مقاوم‌سازی شود.
- ✓ پیکربندی پیش‌فرض تمامی تجهیزات و نرم‌افزارهای مرتبط با سامانه‌های حیاتی تغییر یابد.
- ✓ مستندات مربوط به پیکربندی تجهیزات، سرویس‌ها و سامانه‌های حیاتی بروز شده و در اختیار افراد مجاز قرار گیرد.
- ✓ اعمال هرگونه تغییر در پیکربندی تجهیزات مرتبط با سامانه‌های حیاتی محدود و منوط به کسب مجوزهای لازم و متناسب با سیاست‌های امنیتی سازمان باشد.
- ✓ برای سامانه‌های آسیب‌پذیر مرتبط با سرویس‌های حیاتی، از سیستم‌های خودکار مدیریت وصله‌های امنیتی و یا روش‌های دستی با زمان‌بندی کوتاه استفاده شود و روال کاری مناسبی برای این امر ایجاد شود.

- ✓ تمامی سیستم‌عامل‌ها، سرویس‌ها و سامانه‌های حیاتی به‌صورت مستمر و در بازه‌های زمانی مشخص مطابق با آخرین وصله‌های امنیتی منتشرشده –با احتساب جوانب امنیتی این به‌روزرسانی‌ها– بروز شوند.

۵–۲) امنیت شبکه و سامانه‌ها

- ✓ از دیواره‌های آتش و سامانه مدیریت تهدیدات یکپارچه دارای مجوز در لبه شبکه و سامانهDLP[1] برای کنترل دسترسی، کنترل ترافیک ورودی و خروجی، جلوگیری از نفوذ و جلوگیری از نشت اطلاعات استفاده شود.
- ✓ هر سرویس و خدمتی که در بستر اینترنت ارائه می‌شود باید توسط تجهیزات امنیتی نظیر دیواره آتش، سامانه تشخیص و جلوگیری از نفوذ، دیواره آتش برنامه‌های کاربردی، سامانه ضدبدافزار، ابزارهای کنترل صحت و یکپارچگی فایل‌ها و... محافظت شود.
- ✓ سازمان باید از فعال و بروز بودن تمامی سامانه‌های ضدبدافزار و ضدباج افزار و سامانه تشخیص و جلوگیری از نفوذ در سرور سامانه‌های حیاتی سازمان اطمینان یابد.
- ✓ انتشار سرویس‌های غیرضروری در اینترنت محدود شود.
- ✓ سرویس‌ها و تجهیزات بدون استفاده و غیرضروری مرتبط با سامانه‌های حیاتی در سازمان شناسایی و غیرفعال شوند.
- ✓ همگام‌سازی زمان در تمامی تجهیزات، سامانه‌ها و لاگ‌های مرتبط با سامانه‌های حیاتی رعایت شود.
- ✓ در معماری شبکه باید تفکیک منطقی[2] و ناحیه‌بندی[3] به‌صورت دقیق و مناسب انجام شود و ارتباط ناحیه DMZ با شبکه داخلی توسط دیواره آتش کنترل شود.
- ✓ شبکه متصل به اینترنت از شبکه ارائه سرویس‌های حیاتی سازمانی به‌صورت فیزیکی و یا منطقی (در صورت امکان) جداسازی شود.
- ✓ استفاده از تجهیزات قابل‌حمل شامل رسانه‌های ذخیره‌ساز، تجهیزات سیار سازمانی و شخصی (نظیر لپ‌تاپ، تبلت و...) مدیریت و کنترل شود.
- ✓ محیط‌های تست، توسعه و عملیاتی سامانه‌های حیاتی از یکدیگر جدا شوند.
- ✓ سرور پایگاه داده از سرور برنامه کاربردی سامانه‌های حیاتی جدا شده و دسترسی به آن کنترل شود.
- ✓ استفاده از سرویس میزبانی[4] خارج از کشور برای تمامی سرویس‌ها و سامانه‌های حیاتی غیرمجاز است.
- ✓ از پروتکل‌های امن و ابزارهای رمزنگاری برای حفظ محرمانگی و یکپارچگی داده‌ها و اطلاعات حساس سامانه‌های حیاتی در حین انتقال، پردازش و ذخیره‌سازی استفاده شود.
- ✓ حتی‌الامکان از شبکه بی‌سیم در سازمان استفاده نشود در غیر این‌صورت تمهیدات امنیتی مناسب برای امن‌سازی و مدیریت دسترسی این شبکه‌ها در نظر گرفته شود.

[1] Data Leakage Prevention
[2] Vlan
[3] Zone
[4] Hosting

۶-۲) پایش و مدیریت لاگ

- ✓ رویدادهای امنیتی سامانه‌ها و سرویس‌های حیاتی به‌طور منظم پایش شده و لاگ مرتبط با این سامانه‌ها مدیریت شود (جمع‌آوری، نگهداری، ذخیره‌سازی و اطمینان از صحت عملکرد آن‌ها).
- ✓ لاگ‌های جمع‌آوری‌شده از تمامی سامانه‌ها، به‌منظور کشف ناهنجاری‌ها و حملات سایبری مورد تحلیل قرار گیرند.
- ✓ لاگ‌های ثبت‌شده حداقل برای بازه زمانی یک سال در سازمان نگهداری شود و به‌طور متمرکز در دسترس باشد.
- ✓ لاگ‌های ثبت‌شده در مکان‌های امن و محافظت‌شده نگهداری شوند و در مقابل دسترسی غیرمجاز محافظت شوند.
- ✓ پروتکل‌ها و برنامه‌های کاربردی مرتبط با سامانه‌های حیاتی به‌طور منظم مورد پایش قرار گیرد تا از مطابقت آن‌ها با سیاست‌های امنیتی سازمان (لیست نرم‌افزارها و پروتکل‌های مجاز تهیه‌شده) اطمینان حاصل شود.

۷-۲) تداوم و پایداری سرویس‌ها

- ✓ برای تمامی سرویس‌ها و سامانه‌های حیاتی طرح‌های تداوم و بازیابی از فاجعه تدوین و به‌روزرسانی شود.
- ✓ برای تمامی سامانه‌های حیاتی و سامانه‌های درگیر، داده‌های عملیاتی و حساس باید (مطابق با سازوکار پشتیبان‌گیری که از قبل ایجادشده) نسخه‌های پشتیبان تهیه شود که به‌صورت امن نگهداری می‌شود و از بازیابی آن‌ها در زمان بحران اطمینان حاصل شود.
- ✓ نسخه‌های پشتیبان باید بعد از امن‌سازی سامانه‌ها[۱] و از آخرین وضعیت آن‌ها (آخرین نسخه پیکربندی‌شده) تهیه شود.
- ✓ از وجود تمامی سامانه‌های حیاتی در سایت پشتیبان با عملکرد صحیح، آخرین پیکربندی‌های و داده‌های اطلاعاتی اطمینان حاصل شود.
- ✓ دسترس‌پذیری سامانه‌ها و سرویس‌های حیاتی از طریق راهکارهای توزیع بار، HA و ... افزایش یابد.
- ✓ فهرستی از نهادهای ذیصلاح و افراد کلیدی که باید در زمان بحران در دسترس باشند به همراه اطلاعات تماس آن‌ها، تهیه و بروز شده و در اختیار افراد مجاز قرار گیرد. (در لیست مذکور نفر مرتبط با سازمان، در مرکز افتا حتماً در نظر گرفته شود)

۸-۲) امنیت در زنجیره تأمین

- ✓ SLA مناسب با فراهم‌کننده زیرساخت درزمینهٔ دسترس‌پذیری و تأمین امنیت سرویس وجود داشته باشد.
- ✓ تنها از شرکت‌های دارای مجوزهای امنیتی لازم از مرکز افتا برای دریافت خدمات امن سازی و مشاوره استفاده شود.
- ✓ در خرید تجهیزات افتایی و فاوایی تنها از محصولاتی که دارای مجوزهای امنیتی لازم از مرکز افتا هستند استفاده شود.
- ✓ استفاده از افراد دو تابعیتی در امورات مرتبط با امنیت و مشاغل حساس مجاز نیست.
- ✓ اسامی و سمت افراد دو تابعیتی در جایگاه مدیریتی و کارشناسی به حراست سازمان ارسال شود.

[۱] Hardening

۳) اقدامات زمان بحران

به‌منظور مدیریت صحیح حوادث امنیتی، اقدامات تنها محدود به زمان وقوع حادثه و پس از نمی‌شود. بلکه مجموعه‌ای از تمهیدات پیش از وقوع حادثه باید در نظر گرفته شوند تا آمادگی اولیه در سطح سازمان وجود داشته باشد. در ادامه تشریح اقدامات ارائه‌شده است.

۳–۱) اقدامات قبل از حادثه (آمادگی)

اقدامات قبل از وقوع حادثه سایبری، از نوع اقدامات آماده‌سازی محیط و تیم است که بسترهای مناسب برای مواقع بحرانی را فراهم می‌کند. این اقدامات شامل:

- ✓ انجام اقدامات پیشگیرانه که در بخش ۲ ارائه شد.
- ✓ آموزش کارکنان در راستای فرهنگ‌سازی امنیت
- ✓ تشکیل و آماده‌سازی تیم پاسخ به حادثه (به همراه آموزش و تعریف مأموریت)
- ✓ آماده‌سازی و به‌روزرسانی نرم‌افزارها و سخت‌افزارهای موردنیاز در فرآیند پاسخ به حادثه
- ✓ ایجاد بستر در سازمان هدف برای پاسخ به حادثه و وجود روال‌های اداری و سازمانی هماهنگ و تعریف‌شده در برخورد با حوادث

۳–۲) اقدامات زمان حادثه (شناسایی، مهار، پاک‌سازی، بازیابی)

در این زمان حادثه سایبری صورت گرفته و تیم پاسخگویی به حوادث سایبری باید واکنش سریع و مناسب نشان دهد. مجموعه اقدامات مربوط به قبل از اعزام، حضور در محل حادثه، پاسخ به حمله و ترک محل حمله در این دسته قرار می‌گیرند. اصول زیر در زمان حادثه باید رعایت شود:

- ✓ در صورت مشاهده رخدادهای امنیتی بلافاصله مرکز افتا در جریان امر قرار گیرد.
- ✓ در صورت نیاز به هرگونه قطعی در هر یک از سرویس‌های حیاتی، هماهنگی‌های لازم با مرکز افتا صورت گیرد.
- ✓ محدوده حادثه و بحران را مشخص شود.
- ✓ دیاگرام شبکه و توپولوژی ارتباطات بین سیستم‌ها توسط مسئولین مشخص شود.
- ✓ براساس دیاگرام شبکه، نوع و اهمیت سرویس‌ها و همچنین نوع حادثه، ارتباطات شبکه‌ای محدود شود. ممکن است براساس وسعت و نوع حادثه ناچار به قطع اینترنت کل سازمان هدف باشید.
- ✓ سیستم‌های حساس از نظر داده و سرویس را با کمک مسئولان سازمان اولویت‌بندی شود.
- ✓ سیستم‌های آلوده و آسیب‌پذیر را قرنطینه کرده و از شبکه جداسازی شود.
- ✓ عملیات اکتساب داده انجام شده و بعد از اکتساب داده عملیات بازیابی شروع شود.
- ✓ عملیات فورنزیکی و بازیابی از سیستم‌های با اولویت بالا شروع شود.
- ✓ هرگونه لاگ در مسیر ارتباطی بین سیستم تا اینترنت از قبیل لاگ دیواره آتش، IDS و ... جمع‌آوری شود.
- ✓ اگر سیستم به اینترنت وصل باشد در این صورت کابل شبکه از سیستم جدا شود.
- ✓ هر چیز غیرعادی حین بررسی مستند شود.
- ✓ از ابزارها و افراد نامطمئن برای مهار استفاده نشود.

- ✓ با افراد حاضر در صحنه حادثه (مخصوصاً مدیر سیستم) مصاحبه بعمل آید.
- ✓ هیچ‌گونه اطلاعات فنی تا زمان پایان پاسخ به حادثه در اختیار افراد فاقد صلاحیت قرار داده نشود.
- ✓ همه نکات یادداشت شده و هیچ چیزی تغییر داده نشود.
- ✓ وضعیت سیستم قبل از جمع‌آوری شواهد تغییر داده نشود (اجتناب از به‌روزرسانی، ترمیم و بازیابی و خاموش نمودن سیستم).
- ✓ مطمئن شوید که فرد غیرمجاز و مظنون نمی‌تواند به داده‌ها به‌صورت فیزیکی یا از طریق شبکه دسترسی داشته باشد.
- ✓ تجهیزات ذخیره‌سازی داده‌ها از میدان‌های مغناطیسی، گردوخاک و شوک الکتریکی محافظت شوند.
- ✓ داده‌های حساس، شکننده و فرار بدون آسیب زدن به حافظه‌های غیرفرار منتقل شوند.
- ✓ از هارددیسک قربانی برای ذخیره‌سازی شواهد استفاده نشود.
- ✓ محل ذخیره داده‌های اکتساب شده به‌صورت فیزیکی امن باشند.
- ✓ به شواهد جمع‌آوری‌شده برچسب زده شود.
- ✓ زنجیره نگهداری و انتقال شواهد مستندسازی شده و شواهد در اختیار افراد فاقد صلاحیت قرار داده نشود.

رویه نگهداری و امحاء شواهد جمع‌آوری‌شده از سازمان باید تعیین شود و اصول زیر رعایت شود:

- ✓ مشخصات فرد و زمان و اهداف دسترسی به شواهد یادداشت شوند.
- ✓ روی رسانه اصلی چیزی نوشته نشود.
- ✓ هیچ پردازه‌ای را از بین نبرید.
- ✓ به زمان سیستم دست نزنید.
- ✓ از شواهد محافظت کنید (هیچ مدرکی نباید در فرآیند انتقال و بررسی از بین برود)
- ✓ شواهد را آلوده نکنید (هیچ بدافزاری نباید در حین آنالیز وارد سیستم شود)
- ✓ در بررسی شواهد، نکات اخلاقی رعایت شوند.
- ✓ با ابزارهای نرم‌افزاری و سخت‌افزاری مناسبی ایمیج تهیه شود.
- ✓ هش ایمیج بدست آمده با هش اطلاعات اصلی مقایسه شده تا نسبت به صحت داده‌ها اطمینان حاصل شود.
- ✓ روی داده اصلی کار نشود.
- ✓ در استفاده از رسانه اصلی، عملیات جلوگیری از نوشتن به‌صورت سخت‌افزاری یا نرم‌افزاری اجرا شود.
- ✓ رسانه‌ای که قرار است ایمیج مبدأ روی آن قرار گیرد باید کاملاً خالی باشد.
- ✓ حداقل دو کپی از شواهد تهیه‌شده باشد.

۳–۳) بازیابی سیستم

پس از بروز رخدادهای امنیتی بلافاصله طرح‌های تداوم فعالیت و بازیابی از فاجعه از نظر کارایی موردبررسی قرارگرفته و در صورت نیاز اقدامات مربوطه بعمل آید. عملیات بازیابی اقداماتی را شامل می‌شود که باعث می‌شود که سیستم به حالت نرمال بازگردد و بتواند سرویس‌دهی کند.

- ✓ عامل حادثه (بدافزاری، نرم‌افزاری، سخت‌افزاری، انسانی) شناسایی شود.
- ✓ عامل حادثه را از سیستم‌های پشتیبان و سیستم‌های جاری و در حال کار حذف کنید.
- ✓ سیستم‌عامل و برنامه‌های کاربردی را به‌روزرسانی کنید.

- ✓ ضعف‌های امنیتی شناسایی‌شده روی شبکه از قبیل عدم وجود دیواره آتش، سرویس‌های غیرضروری موجود، عدم وجود آنتی‌ویروس و ... را برطرف کنید.
- ✓ سیستم پشتیبان را به‌روزرسانی کرده و ابتدا به‌صورت آزمایشی در مقابل عامل حادثه تست و ارزیابی کنید.
- ✓ درصورتی‌که سیستم پشتیبان درست کار کرد، آن را راه‌اندازی کنید.
- ✓ رفتار سیستم و رفتار عامل حادثه را تا زمان پایداری سیستم و رفع بحران به‌صورت مناسب و شبانه‌روزی رصد کنید.
- ✓ اگر سیستم‌هایی در سایر قسمت‌های شبکه نسبت به عامل حادثه یا عوامل مشابه دیگر آسیب‌پذیر هستند اقدامات رفع آسیب‌پذیری روی آن‌ها انجام دهید.

۳-۴) اقدامات بعد از حادثه (یادگیری)

- ✓ رویه‌های مناسب یادگیری از حوادث امنیت اطلاعات تدوین و عملیاتی شود تا از تکرار حوادث امنیتی مرتبط جلوگیری شود.
- ✓ ایجاد گزارش حادثه و مستندسازی مناسب آن
- ✓ ارائه راهکار مناسب جهت جلوگیری از تکرار مجدد چنین حوادثی
- ✓ انتقال دانش و تجربیات به سازمان‌ها
- ✓ حفظ و نگهداری شواهد
- ✓ امحای شواهد بعد از زمان مقرر

۴) اقدامات مدیریتی

- ✓ در نظر گرفتن تمهیدات لازم در خصوص مدیریت صحیح منابع انسانی به‌منظور جلوگیری از نارضایتی نیروهای مؤثر
- ✓ حتی‌المقدور ممنوعیت مرخصی‌ها در بازه بحران و یا مرخصی با برنامه‌ریزی متناسب با شرایط
- ✓ وجود فرایندهای تعاملی بین واحدهای امداد سایبری با متولیان سرویس‌ها و سامانه‌ها
- ✓ ایجاد تیم مدیریت بحران، تعیین نقش‌ها و مسئولیت‌ها و شرح وظایف مشخص و مکتوب
- ✓ آموزش افراد کلیدی و اعضای تیم مدیریت بحران به‌منظور مقابله و برخورد مناسب با حوادث سایبری
- ✓ معرفی نماینده تیم مدیریت بحران به‌عنوان مدیر پاسخگویی به رخداد سایبری به‌منظور تعامل و اطلاع‌رسانی حوادث سایبری به مرکز افتا
- ✓ تدوین و اجرای برنامه‌های فرهنگ‌سازی و آگاه‌سازی کلیه کارکنان در حوزه امنیت سایبری
- ✓ آموزش و آگاهی‌رسانی پرسنل در حوزه سیاست‌های امنیتی سازمان و مقابله با مهندسی اجتماعی