سازمان پدافند غیرعامل کشور

فوری

بسمه تعالی
جمهوری اسلامی ایران
فرماندهی کل قوا
ستاد کل نیروهای مسلح

از: سازمان پدافند غیرعامل کشور

شماره: ۳۲۳۲/۱/۲۰۱/۰۰۵۷۰
تاریخ: ۱۴۰۰/۰۸/۲۷
پیوست: دارد.

به: وزیر محترم نفت – برادر ارجمند جناب آقای مهندس اوجی

موضوع: دستورالعمل عملیاتی عملیات پیشگیری (اقدامات اساسی) در زمان هشدار سایبری

مسئله‌ی پدافند غیرعامل مسئله‌ی بسیار مهمی است و هرروزی که می‌گذرد بر اهمیت پدافند غیرعامل افزوده می‌شود. امام خامنه‌ای (مدظله‌العالی)

سلام‌علیکم؛

با صلوات بر حضرت محمد و آل محمد (ص) و با احترام؛

بدین‌وسیله به پیوست دستورالعمل عملیاتی عملیات پیشگیری (اقدامات اساسی) در زمان هشدار سایبری جهت بهره‌برداری و ابلاغ به دستگاه‌های تابعه آن وزارت خانه محترم ارسال می‌گردد.

رئیس سازمان پدافند غیرعامل کشور
سرتیپ پاسدار دکتر غلامرضا جلالی

رونوشت:
معاون محترم انرژی سازمان پدافند غیرعامل کشور جهت پیگیری عملیاتی آن.

ستاد وزارت نفت-
سیستم یکپارچه اتوماسیون اداری
شماره نامه: ۳۳۹۶۱۲
تاریخ ثبت: ۱۴۰۰/۸/۲۹

وصول از طریق اتوماسیون اداری
تاریخ ۱۴۰۰/۸/۳۰

سازمان پدافند غیرعامل کشور

فوری

جمهوری اسلامی ایران
فرماندهی کل قوا
ستاد کل نیروهای مسلح

شماره: ۳۲۳۲/۱/۲۰۱/۰۰۵۷۰
تاریخ: ۱۴۰۰/۰۸/۲۷
پیوست: دارد. (۱۲ صفحه)

از: سازمان پدافند غیرعامل کشور

به: وزیر محترم نفت – برادر ارجمند جناب آقای مهندس اوجی

موضوع: دستورالعمل عملیاتی عملیات پیشگیری (اقدامات اساسی) در زمان هشدار سایبری

مسئله‌ی پدافند غیرعامل مسئله‌ی بسیار مهمی است و هرروزی که می‌گذرد بر اهمیت پدافند غیرعامل افزوده می‌شود. امام خامنه‌ای (مدظله‌العالی)

سلام‌علیکم؛

با صلوات بر حضرت محمد و آل محمد (ص) و با احترام؛

بدین‌وسیله به پیوست دستورالعمل عملیاتی عملیات پیشگیری (اقدامات اساسی) در زمان هشدار سایبری جهت بهره‌برداری و ابلاغ به دستگاه‌های تابعه آن وزارت خانه محترم ارسال می‌گردد.

برادران عالی‌قدر جهانشریک و ولی
جناب آقای غلامپیمان
" " شیراوند
" " صفرزادان
با سلام و احترام جهت اقدام معتمدی
۱۴۰۰/۸/۲۹

رئیس سازمان پدافند غیرعامل کشور
سرتیپ پاسدار دکتر غلامرضا جلالی

رونوشت:
معاون محترم انرژی سازمان پدافند غیرعامل کشور جهت پیگیری عملیاتی آن.

سناد وزارت نفت - ۱۴۰۰/۸/۳۰
سیستم یکپارچه اتوماسیون اداری
شماره نامه: ۳۳۹۶۱۲
تاریخ ثبت: ۱۴۰۰/۸/۲۹

وصول از طریق اتوماسیون اداری و ... تاریخ ۱۴۰۰/۸/۳۰

دبیرخانه هیئت مدیره شرکت ملی صنایع پتروشیمی تاریخ ۱۴۰۰/۸/۳۰ شماره ۶۲۳۴۷

دستورالعمل عملیاتی

عملیات پیشگیرانه (اقدامات اساسی) در زمان هشدار سایبری

قرارگاه پدافند سایبری کشور

آبان ۱۴۰۰

بسم الله الرحمن الرحیم

مقدمه:

فضای سایبری و فناوری های پیشرفته مربوط به آن، هرچند مزایا و مواهب زیادی برای کاربران فراهم می کنند، در عین حال بستر مناسبی نیز برای مهاجمان در جهت تدارک حملات سایبری بوجود می آورند. در میان حملات سایبری که هر روز انجام می شود، آن دسته از حملاتی که با هدف اختلال و تخریب عملکرد زیرساخت های حیاتی، حساس و مهم کشور صورت می گیرد، از اهمیت بسیار زیادی برخورداراست و توجه خاص و عنایت ویژه همه دست اندرکاران را برای انجام عملیات پیشگیری و مقابله می طلبد. استمرار خدمات اساسی زیرساخت ها و سامانه های کشور و پایدارسازی عملیاتی آنها تا حد زیادی مرهون اقدامات پیشگیرانه ای است که در زمان هشدار سایبری صورت داده می شود و می تواند میزان آسیب ها و صدمات وارده و نیز زمان توقف احتمالی خدمات اساسی و عملکردهای حیاتی را به حداقل ممکن تقلیل دهد. این دستورالعمل در جهت راهنمایی متولیان زیرساخت های حیاتی، حساس و مهم کشور برای اقدامات اساسی در زمان هشدار سایبری تهیه شده است تا مبنای عمل قرار گیرد.

الف) مرحله آماده باش (در آستانه رخداد)

هدف از این مرحله، تشدید آمادگی های لازم، هشدار به زیرمجموعه ها، ابلاغ آماده باش رسمی به عوامل مدیریت بحران برای مواجهه با حملات سایبری متناسب با تعیین وضعیت سایبری است. در این مرحله، تمام مدیران و کارشناسان بایستی برای مواجهه با حمله سایبری در آمادگی کامل باشند.

برخی از اقدامات در این مرحله عبارتند از:

۱. کمیته مدیریت بحران / کمیته امنیت سایبری؛ بایستی با حضور مستمر اعضا نسبت به پایش اوضاع و حصول اطمینان از وجود آمادگی های لازم، اقدام نماید.

۲. بر صیانت از دارایی ها و سرویس های اولویت دار (بر اساس اصل جذابیت هدف برای دشمن) تمرکز گردد.

۳. نصب سریع و به موقع وصله های امنیتی دریافت شده از سوی مراجع ذی صلاح در دستور کار باشد.

۴. از راهبردها و تاکتیک های مرتبط با فریب مهاجمین سایبری در جهت ایجاد تاخیر در دستیابی به اهداف مورد نظر بهره گیری شود.

۵. تشدید و استمرار اقدامات رصد، پایش، تشخیص و هشدار رخدادها و حملات سایبری بصورت ۷*۲۴ صورت پذیرد. (افراد مستقر در مراکز عملیات امنیت[1] ۲۴ ساعته رصد و پایش امنیتی را انجام دهند)

۶. تشدید رصد و پایش جهت بررسی ترافیک غیرعادی ورودی و خروجی شبکه در DMZ[2]های مختلف و بر روی پروتکل های گوناگون و گزارش دهی مراتب درصورت مشاهده ناهنجاری ها صورت پذیرد.

۷. نقاط اتصال شبکه داخلی به شبکه های بیرونی با اقدامات امنیتی مناسب محدود، کنترل و پایش شود.

۸. تمام دسترسی های راه دور به شبکه زیرساخت با بهره گیری از هر نوع پروتکل و یا تونلی، قطع شود.

۹. از اتصال و برقراری دسترسی از راه دور به هر نحو و با هر شرکت و یا پیمانکار داخلی و خارجی برای پشتیبانی، به روز رسانی و تعمیرات اجزای شبکه ممانعت به عمل آید.

---

[1] Security Operation center (SOC)
[2] Demilitarized Zone

۱۰. بازبینی پیکره بندی امن تمام اجزای شبکه بالاخص اجزای حیاتی مانند سویچ ها و راهیاب های اصلی، تجهیزات امنیتی و ... و امن سازی آنها بصورت مستمر مطابق با دستورالعمل‌های موجود صورت پذیرد و از پیکربندی امن تمام تجهیزات، اطمینان حاصل شود.

۱۱. تمام اتصالات نامن بیسیم بین اجزای شبکه برای انتقال اطلاعات (شامل VSAT، Wi-Fi، SIGFOX، LoRa و ...) مسدود شوند.

۱۲. تمامی لاگ‌ها، رخدادها و هشدارها در سطوح مختلف اعم از کاربری، هسته، تجهیزات، ارتباطات و غیره با رعایت اصول پدافندی مانند Signing، Time Stamp، Indexing و غیره در پایگاه داده مناسب ذخیره گردد. بدیهی است یکی از کارکردهای این پایگاه داده، مکانیزم کشف منشا حملات[۳] است.

۱۳. سیاست های امنیتی مناسب برای دسترسی افراد بالاخص افرادی که دارای سطح دسترسی به اجزای کلیدی شبکه می باشند؛ با فرض ایجاد و ارتقای محدودیت ها و با اولویت پایش و کنترل اقدامات انجام شده توسط مدیران شبکه، تدوین، ابلاغ و اجرا شود.

۱۴. از تجهیزات رایانه‌ای مشخص، از قبل تعریف شده، امن سازی نرم افزاری، سخت افزاری و میان افزاری شده و احراز صلاحیت شده از سوی حراست زیرساخت، برای اتصال به شبکه جهت عیب یابی، به روزرسانی، تعمیرات و ... استفاده شود.

۱۵. تشدید اقدامات کنترلی و محدود سازی دسترسی افراد به سامانه ها و رعایت حفاظت فیزیکی برای بخش های حساس شامل مراکز ورودی، مراکز داده، Server Roomها و حضور پیمانکاران صلاحیت دار در زیرساخت اجرایی شود.

۱۶. تمام تیم های واکنش به شرایط اضطراری (CSIRT) در آماده باش کامل عملیاتی باشند.

---

[۳] Forensic

۱۷. سامانه های شبکه و بطور اخص سامانه های امنیتی مورد استفاده مانند ضدبدافزار، سامانه تشخیص/اجلوگیری از نفوذ و ... بصورت امن به روز رسانی شوند و مدیریت وصله به صورت ایمن پیاده سازی شود.

۱۸. در پیکره بندی شبکه و اجزای آن تمهیداتی اجرایی شود تا تمام دسترسی ها به شبکه در داخل کشور و از طریق زیرساخت و پهنای باند در اختیار کشور با اولویت شبکه ملی اطلاعات مسیریابی شود. (Iran Access)

۱۹. تمام اقدامات اجرایی جهت استفاده از سازوکار H.A.[۴] و ارتقاء و عملیاتی نمودن افزونگی[۵] در اجزای کلیدی شبکه پیاده سازی شود.

۲۰. تمام نام های کاربری و گذرواژه های اجزای شبکه و بطوراخص اجزای کلیدی آن به سرعت با نام کاربری و گذرواژه امن جدید جایگزین شود.

۲۱. توصیه اکید می شود تا بازنگری معماری امنیتی و پدافندی شبکه در تمام سطوح اعم از سطح کاربری، سطح هسته شبکه، سطح ارتباطات بر اساس معماری امن و لایه به لایه مبتنی بر دفاع در عمق صورت پذیرد و اقداماتی مانند تغییر برخی از پیکربندی های تجهیزات جهت اختلال و وقفه در مسیر تهجم اجرا شود. (اصل برهم زدن صحنه درگیری)

۲۲. افزایش تعدد نوبت های پشتیبان گیری امن بصورت بلادرنگ از سامانه ها و پایگاه داده‌های حیاتی و ذخیره سازی داده ها و اطلاعات آنها بصورت Online و Offline در دستور کار باشد.

۲۳. تمام پشتیبان ها در حالت عملیاتی و قابل استفاده برای موارد ضروری باشد.

۲۴. تمام باتری ها، UPSها و ژنراتورها عملیاتی و قابل استفاده باشند.

---

[۴] High Availability
[۵] Redundancy

۲۵. تمهیداتی جهت آماده سازی تجهیزات یدک به منظور جایگزینی سریع در شرایط اضطراری اجرا شود. (تجهیزاتی که همانند تجهیز اصلی پیکربندی و برنامه ریزی شده اند تا سریعا جایگزین تجهیز اصلی آسیب دیده شود).

۲۶. تمهیداتی اجرا گردد تا در صورت قطع و یا اختلال در سرویس GPS، همزمان سازی از طریق سازوکار امن دیگر صورت پذیرد و خللی در خدمات اساسی زیرساخت ایجاد نگردد.

۲۷. تمهیداتی اجرایی گردد تا حراست زیرساخت بر روند ورود و خروج نیروها اعم از کادر سازمانی و پیمانکاران که سطح دسترسی بالایی در شبکه دارند کنترل و نظارت جدی داشته باشد.

۲۸. درصورت بروز هرگونه رخداد غیرطبیعی در شبکه (اعم از سایبری یا غیرسایبری) در اسرع وقت مراتب به سازمان پدافندغیرعامل کشور گزارش شود.

در خصوص وجود آسیب پذیری سطح بالا در واسط ILO در درگاه های سرورهای HP لازم است اقدامات زیر اجرایی شود:

۱. دسترسی به پورت ILO بسیار محدود شده و دسترسی از طریق شبکه اینترنت و شبکه های ناامن به این درگاه بطور کامل مسدود شود. دسترسی از شبکه داخلی به درگاه بسیار محدود و یا بطور کامل قطع گردد.

۲. قابلیت DHCP Client سرور غیرفعال گردد تا در صورت اتصال پورت به صورت غیر عمد، از دریافت آدرس IP اجتناب شود.

۳. تمامی دسترسی های سطح ادمین به اکتیودایرکتوری مورد بازبینی قرار گرفته و پسوردهای قبلی اکانت‌های ادمین به سرعت تغییر نماید.

۴. نسبت به قرارگیری اسکریپت لاگین و استارتاپ حساس بوده و این موارد بررسی گردد.

۵. تمامی دسترسی های سطح روت به سرورهای ESX، Xen ، انواع Linux و انواع ویندوز سرورهای نصب شده بر روی سرورهای فیزیکی مورد بازبینی قرار گرفته و رمز اکانت های روت/ ادمین بازنشانی گردد.

۶. سرویس SSH را در سرورهای ESX غیرفعال شود.

۷. دسترسی از راه دور به شبکه محدود گردد و از روش های امن و رمز نگاری مناسب استفاده شود.

۸. مرکز رصد، پایش، تشخیص و هشدار (SOC) بصورت ۲۴*۷ فعال باشد و هرگونه رخداد مشکوک را به سرعت شناسایی، کنترل و مدیریت نمایند و بلافاصله با سازمان پدافند غیرعامل کشور اطلاع داده شود.

۹. تجهیزات امنیتی بالاخص دیوار آتش، سامانه های تشخیص / جلوگیری از نفوذ و سامانه مدیریت اطلاعات و رخدادهای امنیتی (SIEM) نسبت به تلاش برای دسترسی به پورت‌های ILO یا SSH به سرورها و دسترسی‌های ریموت خارج سازمان حساس بوده و موارد هشدار با اولویت پیگیری شود.

۱۰. نسبت به تهیه پشتیبان منظم از داده‌ها بر روی رسانه‌های آفلاین و اطمینان از صحت پشتیبان‌ها اقدام گردد.

ب) مرحله مقابله (حین رخداد)

هدف اصلی در این مرحله، **مدیریت صحنه عملیاتی، خنثی سازی تهاجم، انسداد و انحراف مسیرهای تهاجم، کاهش صدمات و خسارات ناشی از تهاجم سایبری، جلوگیری از گسترش دامنه حملات به بخش‌های دیگر، تعیین منشا حمله و مشخصات مهاجم است.**

- به محض بروز حادثه به سرعت و در کوتاه ترین زمان، مراتب توسط مسئولین مستقیم دستگاه آسیب دیده به سازمان پدافندغیرعامل کشور اطلاع رسانی شود. کانال های اطلاع رسانی مختلف در پیوست شماره ۱ این دستورالعمل آورده شده است.
- مدیریت صحنه عملیات در سطح کلان بر عهده مدیرعامل/ رئیس زیرساخت مربوطه می باشد.
- به منظور جمع آوری کامل شواهد و مستندات و ادله مثبته توسط تیم های اعزامی از مراکز حاکمیتی در حوزه امنیت و پدافند سایبری، از تغییر در صحنه/صحنه های حمله سایبری اجتناب شود.

برای دفاع از سرمایه های سایبری و وابسته به سایبر، اقدامات زیر انجام پذیرد:

- کمیته مدیریت بحران بصورت مستمر فعال بوده و بر اساس گزارش‌های دریافتی از صحنه عملیات، اقدامات و تصمیمات مقتضی را اتخاذ و اقدام نماید از قبیل :
- دفاع[۶] و ممانعت[۷] از گسترش حمله با بکارگیری روش های استاندارد و دستورالعمل های صادر شده
- ایزوله نمودن قسمت های آسیب دیده از سایر قسمت های شبکه

---

[۶] Defend
[۷] Deny

۱. ثبت تمامی لاگ‌ها (در صورت امکان)، رخدادها و هشدارهای تولید شده حاصل از تهاجم سایبری، در پایگاه داده و با رعایت استانداردهای ثبت لاگ، به منظور بهره برداری در عملیات Forensic

۲. کنترل و کاهش شدت تهاجم سایبری از طریق:

ب) خارج کردن بخشی از سامانه / شبکه از دسترس (در صورت امکان)

ت) محدودسازی پهنای باند

ث) محدودسازی و قطع مسیر دسترسی (در صورتیکه حمله سایبری در بخش غیرصنعتی می باشد)

ج) خارج کردن برخی از سرویسها (در صورتیکه حمله سایبری در بخش غیرصنعتی می باشد)

۳. در صورت امکان فریب مهاجم با استفاده از مکانیزم هایی مانند Honeypot و Honey net در دستور کار قرار گیرد.

۴. قرنطینه سازی عوامل بدافزاری در دستور کار قرار گیرد.

۵. شروع عملیات پاکسازی بلافاصله پس از مشاهده رفتارهای بدافزاری مخرب با رعایت موارد امنیتی انجام شود.

۶. تهیه Image از پیکربندی شبکه های صنعتی و غیرصنعتی (IT/OT) انجام شود.

۷. تغییر پویای محدوده IPهای سرویس های مورد حمله واقع شده در شبکه غیرصنعتی صورت پذیرد.

۸. رعایت احتیاط کامل در استفاده از وصله‌های امنیتی به منظور پوشاندن آسیب پذیری‌های شبکه اجرایی شود.

۹. ارسال صحیح نمونه‌های آلوده به مراجع بالادستی برای بررسی بیشتر صورت پذیرد.

۱۰. اطلاع رسانی سریع به مراجع ذیصلاح درصورت مشاهده حمله سایبری انجام شود.

۱۱. اطلاع رسانی مناسب و به هنگام به تمام افراد دخیل و در سطوح مختلف داخلی زیرساخت انجام شود.

۱۲. آمادگی کامل برای همکاری با تیم های اعزامی از سازمان های حاکمیتی در حوزه امنیت و پدافند سایبری وجود داشته و عملیاتی شود.

ج) مرحله بازیابی (پس از رخداد)

پس از وقوع حمله سایبری باید اقدامات لازم برای **بازیابی شرایط عادی و تداوم عملکرد، به سرعت اجرایی شود** و زمان از دسترس خارج شدن زیرساخت، به حداقل ممکن کاهش یابد. مدیریت رخداد سایبری، کاهش خسارات ناشی از حمله و پرهیز از پیامدهای فاجعه‌بار در این مرحله انجام می شود.

برخی از مهمترین اقدامات این مرحله عبارتند از :

۱. انجام بازیابی و بازسازی سیستم های آسیب دیده با رعایت ملاحظات امنیتی صورت پذیرد.

۲. تحلیل و ارزیابی ابعاد، منشاء، شدت و پیامد حادثه و حصول اطمینان از ایذایی یا واقعی بودن حمله انجام شده در دستور کار باشد.

۳. برآورد خسارات وارد آمده به سامانه های آسیب دیده و گزارش آن به مبادی ذیربط انجام شود.

۴. ممانعت از انتشار آلودگی سیستم های آسیب دیده به سایر سیستم ها اجرایی شود.

۵. شناسایی مهاجم و روش بکارگرفته شده (ابعاد، منشاء و پیامد) با کمک و راهبری مراجع ذیصلاح عملیاتی شود.

۶. مستندسازی ادله و شواهد قانونی طبق متدولوژی های پیش گفته با کمک مراجع ذیصلاح انجام شود.

۷. همکاری موثر در پیگیری حقوقی تهاجم از مسیرهای قانونی اجرایی شود.

۸. در صورت امکان رعایت اصل سایه سازی[۸] با ایزوله سازی و تست سامانه های آسیب دیده به منظور حصول اطمینان از رفع کامل آلودگی و قبل از بکارگیری مجدد در شبکه انجام شود.

۹. مستندسازی و انتقال تجربه رخدادهای به وقوع پیوسته به عنوان آموخته های حاصل از رخدادها و حملات سایبری مشابه در دستور کار قرار گیرد.

۱۰. قبل از شروع مجدد مرحله عملیاتی، آزمون های لازم برای حصول اطمینان از عملکرد صحیح سیستم و حذف کامل عوامل تهاجم، انجام شود.

---

^ Shadowing

پیوست شماره یک

کانال های اطلاع رسانی دستگاه های آسیب دیده از رخدادهای سایبری به سازمان پدافند غیرعامل کشور:

- **شبکه دولت برای ارسال و دریافت نامه ها و مکاتبات**
- **شماره نمابر ۲۵۹۳۵۴۸۳**
- **شماره تلفن ثابت ۲۵۹۳۵۳۳۳**
- **خط تلفن همراه ۰۹۱۲۲۹۹۴۸۲۸ مهندس هادی کریمی**
- **خط تلفن همراه ۰۹۱۲۶۵۹۹۰۱۸ مهندس خالق گرجی**
- **خط تلفن همراه ۰۹۱۶۱۴۰۰۶۲۱ برادر خوانساری**