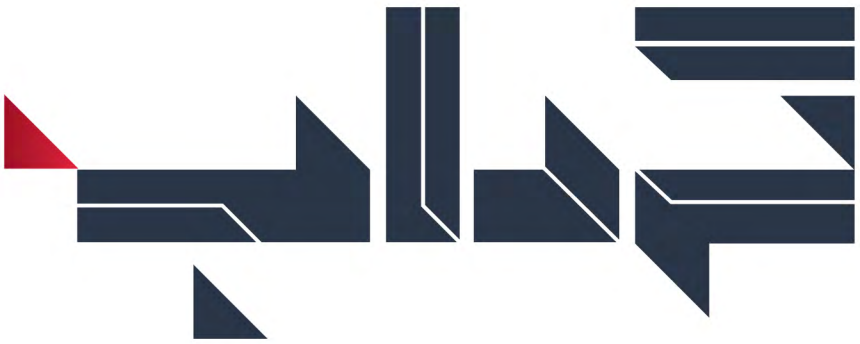
اهداف اجرایی امنیت سایبری ایالات متحده آمریکا

متن کامل قانون

بسم الله الرحمن الرحيم



حکمرانی سایبری و حفظ زیرساخت‌های حیاتی

با پیچیده‌تر و خطرناک‌تر شدن حملات سایبری، تهدیدات علیه زیرساخت‌های حیاتی آمریکا روز به روز افزایش می‌یابد و امنیت ملی، امنیت کسب‌وکارها و امنیت مردم را به خطر میاندازد. وزیر امنیت داخلی ایالات متحده آمریکا، الهاندرو مایورکاس، در سخنرانی اخیر خود به این موضوع اشاره کرد. او به سیاستمداران و مردم هشدار داد که وقتی یک هکر از هر کجای جهان می‌تواند با فشار دادن یک کلید اقدام به حمله سایبری کند، به این معنی است که امنیت ملی و امنیت داخلی مورد تهدید قرار دارند و این دو اساساً مترادف هم هستند. او گفت: «فناوری های پیشرفته و قابل دسترس، بی‌ثباتی اقتصادی و سیاسی، اقتصاد جهانی و بدون مرز باعث افزایش تهدیدات و چالش‌ها برای جوامع ما از جمله مدارس، بیمارستان‌ها، کسب‌وکارهای کوچک، دولت‌های محلی و زیرساخت‌های حیاتی شده است».

پیامد حملات سایبری در سازمان‌های مربوط به زیرساخت‌های حیاتی مانند تأسیسات برق، کارخانه‌های تصفیه آب، تولیدکنندگان مواد شیمیایی و بیمارستان‌ها فاجعه بار است. برای مثال، زمانی که هکرها به شبکه برق اوکراین حمله کردند صدها هزار نفر به مدت چند روز بدون برق زندگی کردند یا زمانی که گروه‌های باج‌افزار به یک بیمارستان حمله کردند، بیمارستان مجبور شد تا سیستم نوبت‌دهی خود را به حالت آفلاین دربیاورد و به این ترتیب بیماران از خدمات مراقبتی لازم محروم ماندند. یکی از بدترین موارد، حمله باج‌افزار به سیستم شرکت کلونیال پایپ لاین (Colonial Pipeline) بود که باعث شد بسیاری از شهروندان آمریکایی با مشکل تأمین سوخت برای وسایل نقلیه مواجه شوند.

با توجه به روند رو به رشد این نوع تهدیدات، حال دولت آمریکا به دنبال آن است تا در استراتژی‌های امنیت سایبری خود تجدیدنظر کند و اهداف عملکرد امنیت سایبری که اخیراً سرویس امنیت سایبری و امنیت زیرساخت (CISA) آن را منتشر کرده است، چارچوب مناسبی برای انجام این کار ارائه می‌دهد.

برای سازمان‌هایی که به دنبال ایجاد تغییر و تقویت امنیت سایبری شبکه‌های فناوری اطلاعات و عملیاتی خود هستند، استفاده از فهرست تلفیقی و جامع از بهترین شیوه‌ها و توصیه‌ها درباره مفاهیم مختلف از جمله زیرو تراست، لایه دفاعی عمیق، تقسیم‌بندی‌ها، مدیریت دارایی و توجه به اهداف مشخص شده از سوی سرویس امنیت سایبری و امنیت زیرساخت آمریکا (CISA) می‌تواند نقطه شروعی مناسبی باشد.

سطوح حمله در بخش‌های زیرساخت‌های حیاتی پیچیده است. برای مثال همه‌گیری کرونا راه‌های جدیدی را برای ارائه خدمات مراقبتی به بیماران ایجاد کرد و باعث گسترده‌تر شدن اتصالات و ارتباطات، بیش از هر زمان دیگری شد. با این که این امر مزایایی برای بیماران و ارائه‌دهندگان خدمات مراقبتی داشت اما سازمان‌های بهداشتی و درمانی در معرض خطرات جدید در سطوح گسترده‌تری قرار گرفتند. آن‌ها می‌بایست از سطح گسترده تری در برابر حملات و تهدیدات محافظت می‌کردند که کار راحتی نبود، چون دیگر مثل گذشته سیستم‌های OT از بخش IT جدا نبودند و ابزارهای سایبری سنتی به دلیل متصل نبودن به هم نمی‌توانستند کمک چندانی کنند.

این قانون می‌تواند به قانون‌گذاران و کارشناسـان حوزه امنیت سـایبری کشـور نیز مطالبی را یادآوری کند. باید همواره در نظر گرفت که پذیرش سـریع فناوری و خدمات ابری هم آن‌چنان بی‌دردسـر نیسـت. استفاده از مدل‌های مبتنی بر فضای ابری راحت و کارآمد به نظر می‌رسـد اما از آن‌جایی که فروشـندگان به عنوان اشـخاص ثالث آن را مدیریت می‌کنند، درها به روی خطرات جدید باز می‌شوند چرا که بعضی از این اشخاص ثالث تجربه کمی با مقررات امنیتی، ادغام در منابع و سیسـتم‌های داده دارند. یک حمله سـایبری موفقیت‌آمیز به یکی از فروشـندگان خارجی می‌تواند چندین سازمان را به خطر بیندازد.

اولین قدمی که ارائه‌دهندگان خدمات زیرساخت‌های حیاتی باید برای رسیدگی به این نوع چالش‌ها بردارند، این است که با سرویس‌های مدیریت خطر بخش خود سعی کنند فهرستی اولویت‌بندی شده از اقدامات امنیت سایبری لازم ایجاد کنند. به این ترتیب با شناسـایی و اجرای شـیوه‌های پایه و نحوه پیگیری تأثیر و عملکرد آن‌ها می‌توان امنیت سایبری را به میزان قابل توجهی حفظ و تقویت کرد و احتمال مورد حمله قرار گرفتن یک شرکت را کاهش داد. چنین اهدافی به مدیران امنیتی در اولویت‌بندی بر سرمایه‌گذاری روی تغییرات اساسی، کمک شایانی می‌کند.

دومین قدم، سرمایه‌گذاری روی متخصصان این حوزه برای اجرای دستورالعمل‌ها و دستیابی به اهداف موردنظر اسـت که شـامل کارکنان فناوری اطلاعات و سـایبری آموزش دیده می‌شود که می‌توانند اقدامات امنیتی یا تغییرات ایجاد شده در پیکربندی را در سطح سازمانی آزمایش، ارزیابی و اجرا کنند.

هماهنگ بودن بخش صنعت و دولت بسیار مهم است. همه سازمان‌های مربوط به زیرساخت‌های حیاتی باید در ارتباط با سرویس امنیت سایبری و امنیت زیرساخت باشند و از محصولات و راهنمایی‌های این سرویس استفاده کنند.

در ادامه متن کامل این سند ترجمه شده و ارائه می‌شود.

سـطح تهدیدات سـایبری روز به روز گسـترده‌تر می‌شـود و به همین دلیل نیاز شدیدی به داشتن رویکرد دفاعی قـوی وجـود دارد. تهدیدات سـایبری نه تنهـا می‌توانند فعالیت‌هـا را مختل کنند، بلکه می‌تواننـد امنیت اطلاعات حسـاس و مهم، جان افراد و امنیت ملی را به خطر بیندازند. سـازمان‌های مربوط به زیرسـاخت‌های حیاتی با پیش بینـی، برنامه‌ریـزی مناسـب و ایجاد آمادگی در صورت بروز بدترین شـرایط می‌توانند خطـرات را دفع کنند و خود را ایمن نگه دارند.

فهرست

پیش‌زمینه و محتوا

چالش پیش رو

سرویس امنیت سایبری و زیرساخت ایالات متحده (CISA) با همکاری دولت، بخش خصوصی و شرکای بین المللی به طور روزانه، سعی دارد تا اطلاعات بیشتری در رابطه با زیرساخت‌های حیاتی (CI) ایالات متحده و ماهیت تهدیدات به دست آورد. همکاری و تلاش مشترک همه‌ی بخش‌های زیرساخت حیاتی به همراه سرویس‌های مدیریت خطرات آن بخش‌ها (SRMA) و تلاش‌های شرکای دولتی، چه در داخل ایالات متحده و چه در خارج از آن، کمک می‌کند تا سرویس امنیت سایبری و زیرساخت با بررسی الگوها به طور منظم، بخش‌هایی را که نیاز به توجه بیشتر و ضروری‌تری به امنیت سایبری دارند، شناسایی کند. کارشناسان و اپراتورهای زیرساخت حیاتی که در تکمیل این سند همکاری داشته‌اند، مشاهدات مشابهی را ارائه دادند.

نگرانی‌ها از وجود شکاف‌های امنیتی صرفا از جنبه‌ی نظری یا فلسفی نیست. ما تأثیراتی را که این شکاف‌ها می‌گذارند تجربه کرده‌ایم؛ از جمله در حملات باج‌افزار به بخش‌های حیاتی مانند بیمارستان‌ها و مدارس یا کمپین‌های پیچیده در سطح ملی که سازمان‌های دولتی و زیرساخت‌های حیاتی را هدف قرار می‌دادند. بدیهی است که این نوع نفوذها امنیت ملی، امنیت اقتصادی و سلامتی مردم را به خطر می‌اندازد.

طی یک سال گذشته، سرویس امنیت سایبری و زیرساخت با همکاری صدها شریک، هزاران دیدگاه دریافت و داده‌های چند سال را تجزیه و تحلیل کرده است تا برای تهدیدات و خطراتی که چالش‌های بزرگی برای امنیت ملی به وجود می آورند، پاسخی بیابد.

۱. بسیاری از سازمان‌ها هنوز روش‌های امنیتی اساسی را اتخاذ نکرده‌اند. استفاده نکردن از روش‌های امنیتی پایه و مهم مانند احراز هویت چندعاملی (MFA)، گذرواژه‌ی قوی، پشتیبان‌گیری و دیگر اقدامات، باعث می‌شود تا زیرساخت‌های حیاتی به طور مکرر در معرض نفوذهای مخرب سایبری باشد.

۲. به سازمان‌های کوچکتر و متوسط کم‌توجهی می‌شود. سازمان‌هایی که دسترسی محدودی به منابع و برنامه‌های امنیت سایبری دارند، اغلب با چالش‌هایی روبرو می‌شوند که نمی‌دانند از چه روش‌هایی برای تأمین امنیت سایبری بهره ببرند. هرچند منابع موجود مانند چارچوب امنیت سایبری مؤسسه ملی استاندارد و فناوری (NIST) بسیار ارزشمند و مفید است؛ اما سازمان‌های کوچکتر در تشخیص مؤثرترین روش با توجه به وضعیت امنیت سایبری خود با مشکلاتی مواجه می‌شوند.

۳. نبود استانداردها و بلوغ سایبری در بخش‌های زیرساخت‌های حیاتی. ناسازگاری قابل توجهی در پتانسیل امنیت سایبری، میزان سرمایه‌گذاری و شیوه‌های اجرایی پایه در داخل و خارج از بخش‌های زیرساخت‌های حیاتی دیده می‌شود که نهایتا منجر به ایجاد شکاف‌هایی برای سوءاستفاده گران می‌گردد.

۴. امنیت سایبری فناوری عملیاتی (OT) اغلب کم‌ارزش تلقی می‌شود. در حال حاضر، صنعت امنیت سایبری تا حد زیادی روی سیستم‌های فناوری اطلاعات تجاری متمرکز است و موارد تهدیدکننده OT نادیده گرفته می‌شود. به این ترتیب، زیرساخت‌های حیاتی به دلیل متصل شدن بیشتر دستگاه های OT به شبکه در معرض خطر جدی قرار می‌گیرند. با این وجود، بسیاری از نهادهای مرتبط با زیرساخت‌های حیاتی فاقد برنامه‌های کافی برای تأمین امنیت سایبری در زمینه OT هستند به ویژه در جاهایی که مشکلات امنیت سایبری را مختص بخش فناوری اطلاعات می‌دانند. از سوی دیگر، نهاد هایی هم که برنامه‌های امنیت سایبری برای OT دارند، اغلب فاقد ابتدایی‌ترین خطوط دفاعی سایبری برای OT هستند و نمی‌توانند روش‌های مناسب با محیط و شرایط خود را پیدا و اجرا کنند.

مقابله با این چالش: نامه‌ی امنیت ملی ۵

در ژوئیه‌ی ۲۰۲۱ رئیس جمهور آمریکا، جو بایدن، تفاهم نامه امنیت ملی (NSM) ۵ را با محتوای بهبود امنیت سایبری برای سیستم‌های کنترلی زیرساخت‌های حیاتی امضا کرد. بنابراین، سرویس امنیت سایبری و زیرساخت موظف شد تا با هماهنگی مؤسسه‌ی ملی استاندارد و فناوری (NIST) و گروه های مربوطه، اهداف سایبری پایه مشترک برای همه‌ی بخش های زیرساخت‌های حیاتی توسعه دهد. این سند حاوی اهداف عملکرد امنیت سایبری بین بخش‌ها (CPG) است. سرویس امنیت سایبری و زیرساخت ایالات متحده با هماهنگی مؤسسه‌ی ملی استاندارد و فناوری، اهداف را مرتبا به‌روز می‌کند و قرار است از اواخر سال ۲۰۲۲، این سرویس فعالیت خود را با سرویس‌های مدیریت خطر بخش (SRMA) آغاز کند تا اهداف خاص هر بخش را مشخص سازد.

سی‌پی‌جی (CPG) چیست؟

به بیان ساده،سی‌پی‌جی یک زیرمجموعه اولویت‌دار از اقدامات امنیت سایبری آی‌تی (IT) و اوتی (OT) است تا خطرات تهدیدکننده‌ی فعالیت‌های زیرساخت‌های حیاتی و شهروندان آمریکا کاهش یابد. این اهداف برای همه‌ی بخش های زیرساخت‌های حیاتی تعریف می‌شود و اطلاعات مربوط به متداول‌ترین و تأثیرگذارترین تهدیدها، تاکتیک‌ها، تکنیک‌ها و رویه‌های دشمن (TTP) که توسط سرویس امنیت سایبری و زیرساخت و دولت و شرکای صنعتی مشاهده شده‌اند، در اختیارشان قرار می‌گیرد. به این ترتیب، مجموعه‌ای از راهکار های حفاظتی مشترک وجود دارد که همه‌ی نهادهای مرتبط با زیرساخت‌های حیاتی (چه بزرگ و چه کوچک) بهتر است آن را در پیش بگیرند.

سی‌پی‌جی منعکس‌کننده‌ی یک برنامه جامع امنیت سایبری نیست؛ بلکه مجموعه‌ای از اقدامات حداقلی است که سازمان‌ها باید برای کمک به زیرساخت‌های حیاتی آن را اجرا کنند. در واقع سی‌پی‌جی شامل حداقل راهکارها و اقدامات برای کاهش خطرات سایبری است. مهم‌تر از همه این که سی پی‌جی شامل موارد زیر نمی‌شود:

- **جامع:** سی‌پی‌جی شامل تک تک اقدامات امنیت سایبری مورد نیاز برای محافظت از سازمان یا تأمین‌کننده‌ی کامل امنیت ملی و اقتصادی و بهداشت و ایمنی عمومی در برابر همه‌ی خطرات احتمالی نیست. در عوض، فعالیت‌هایی حداقلی و پایه برای تأمین امنیت سایبری و کاهش خطرات است که در تمام بخش‌ها قابل اعمال باشد.
- **برنامه‌ی کامل تأمین امنیت سایبری و مدیریت خطرات:** سی‌پی‌جی انواع رویکردها برای مدیریت یا اولویت‌بندی خطرات را آن طور که در چارچوب امنیت سایبری سرویس امنیت سایبری و زیرساخت آمده است، پوشش نمی‌دهد.
- **فرمان صادر شده از سرویس امنیت سایبری و زیرساخت:** اجباری در کار نیست و سازمان‌ها داوطلبانه از سی پی‌جی پیروی می‌کنند. اختیاری بودن آن باعث می‌شود تا راه اولویت‌بندی بهتر سرمایه‌گذاری‌های امنیتی برای دستیابی به نتایج مهم و حیاتی در چارچوب وسیع‌تری مانند NIST CSF فراهم شود.
- **مدلی مختص گروهی با سطح خاص:** موارد ذکرشده در سی‌پی‌جی برای همه‌ی سازمان‌های مرتبط با CI، صرف‌نظر از طبقه‌بندی و سطح‌بندی‌های مختلف، صدق می‌کند (و با این حال سی‌پی‌جی شامل معیارهایی مانند اثرگذاری، هزینه و پیچیدگی است تا به سازمان‌ها در راستای اولویت‌بندی سرمایه های خود کمک کند).

سی‌پی‌جی به طور منظم هر شش تا دوازده ماه به‌روز می شود. سرویس امنیت سایبری و زیرساخت وبسایتی برای دریافت بازخوردها و ایده‌ها جهت گنجاندن اهداف جدید یا تغییر اهداف فعلی راه‌اندازی کرده است.

معیارهای انتخاب سی‌پی‌جی

همان‌طور که پیشتر اشاره شد، سی‌پی‌جی زیرمجموعه‌ای از اقدامات امنیت سایبری است که با همکاری و بررسی دقیق صنعت، دولت و مشاوران متخصص بر حسب چند معیار انتخاب شده است:

۱. خطرات یا اثر ناشی از تهدیدات متداول بین بخش‌ها و تی‌تی‌پی (TTP) دشمن را مستقیم و به طور قابل توجهی کاهش می‌دهد.

۲. واضح، قابل اجرا و قابل تعریف است.

۳. در شرکت‌های کوچک و متوسط به دلیل سادگی و مقرون به صرفه بودن قابل اجراست.

مثالی از یک سی‌پی‌جی که این معیارها را دارد، از این قرار است: «اطمینان یافتن از این که هیچ یک از سیستم‌های متصل به اینترنت یک سازمان، آسیب‌پذیری‌های قابل بهره برداری و شناخته شده (KEV) نداشته باشد.» این سی‌پی‌جی قابل تعریف و دستیابی است و خطر ناشی از یک تهدید شناخته‌شده را مستقیما کاهش می‌دهد. برعکس، اجرای زیرو تراست (Zero Trust) یک سی‌پی‌جی مناسب نخواهد بود؛ زیرا فعالیتی مبهم، غیرقابل تعریف و اندازه‌گیری است و ممکن است برای سازمان‌های کوچک دردسرساز باشد.

مدل سی‌پی‌جی

سی‌پی‌جی‌های ارائه شده در این سند، در یک مدل بصری نمایش داده می‌شوند تا خوانندگان نه تنها درباره‌ی اهداف، بلکه درباره‌ی پیامدها، خطرات یا تی‌پی‌پی‌هایی که به آن‌ها اشاره شده، این که چه چیزی «خوب» تلقی می‌شود و سایر اطلاعات مهم به درک بهتر و عمیق‌تری برسند. هر هدف از اجزای زیر تشکیل شده است:

اجزای مدل	شرح اجزا
پیامد	پیامد و نتیجه‌ای که هر سی‌پی‌جی در تلاش برای دستیابی است.
خطرات / تی‌تی‌پی موردنظر	الف) مجموعه‌ی اولیه MITRE ATT&CK TTP ب) مجموعه‌ای از خطرات و تهدیدات سازمانی که اثرات یا احتمال بروز آنها در صورت دستیابی به پیامد و نتیجه موردنظر کمتر خواهد بود.
اعمال امنیتی	روش‌هایی که سازمان‌ها باید برای دستیابی به نتیجه و کاهش اثر خطرات و تی‌تی‌پی در پیش بگیرند.
محدوده	مجموعه یا زیرمجموعه دارایی‌هایی که سازمان‌ها باید به اقدامات امنیتی اختصاص دهند.
اقدام پیشنهادی	روش‌های نمونه‌ای که طبق داده‌ها و تلاش‌های سرویس امنیت سایبری و زیرساخت و شرکا، به سازمان‌ها در جهت پیشرفت و دستیابی به اهداف عملکردی کمک می‌کند. این اقدامات مرتبا مطابق با تهدیدها و خطوط دفاعی جدید شناسایی شده به‌روز می‌شود.
مرجع NIST CSF	زیرمجموعه سی‌اس‌اف که بیشتر به اقدامات امنیتی مرتبط است.

تفاوت این‌ها با NIST CSF و استانداردهای دیگر چیست؟

استانداردها و دستورالعمل‌های سایبری زیادی مخصوصا از سوی دولت آمریکا وجود دارد. برای مثال NIST CSF یکی از رایج‌ترین و شناخته‌شده‌ترین چارچوب‌های امنیت سایبری به شمار می‌رود و دولت و CISA، سازمان‌ها را تشویق به بهره مندی از NIST CSF می‌کنند تا برنامه‌ی امنیت سایبری‌ای پایدار و منسجم ایجاد شود. بر اساس بازخورد سهامداران، از سی‌پی‌جی، می‌توان در سازمان‌ها به عنوان بخشی از یک برنامه امنیت سایبری گسترده بر مبنای NIST CSF یا چارچوب‌ها و استانداردهای دیگر استفاده کرد.

۱. راهنمای شروع به کار سریع: کمکی که سی‌پی‌جی‌ها به سازمان‌های فاقد تجربه، فاقد منابع یا ساختار مناسب در زمینه‌ی امنیت سایبری می‌کنند، این است که سازمان‌ها سریعا می‌توانند اقدامات اولیه و پایه‌ی امنیت سایبری را تشخیص دهند و اجرا کنند. بعد از اعمال سی‌پی‌جی یا همزمان با آن، سازمان‌ها می‌توانند از NIST CSF برای ایجاد یک برنامه‌ی مدیریت خطر جامع و اجرای دستورالعمل‌های اضافی NIST اقدام کنند.

۲. اولویت‌بندی و دریافت بودجه: سی‌پی‌جی دارای کاربرگ است (در ادامه بیشتر توضیح داده شده است) که به سازمان های کوچک یا سازمان‌هایی با برنامه‌های نه چندان قوی و پیشرفته‌ی امنیت سایبری کمک می‌کند تا بتوانند اقدامات حفاظتی را بر اساس میزان اهمیت، تاثیرگذاری و هزینه اولویت‌بندی کنند و این اطلاعات را در اختیار مدیران اجرایی (غیرفنی) قرار دهند.

۳. تنظیم NIST CSF: هر اقدام امنیتی در سی‌پی‌جی هماهنگ با زیرمجموعه‌ای از NIST CSF است. لازم به ذکر است که سی‌پی‌جی‌ها به طور کامل به هر زیرمجموعه از NIST CSF نمی‌پردازند. در هر اقدام امنیتی، شناسایی زیرمجموعه‌ی CSF نمایانگر رابطه‌ی بین سی‌پی‌جی و NIST CSF است. سازمان‌هایی که قبلا NIST CSF را اجرایی کرده‌اند، نیازی به انجام کارهای اضافی برای اجرای سی‌پی‌جی‌های مربوطه نخواهند داشت.

نحوه‌ی استفاده از سی‌پی‌جی

محتویات سی‌پی‌جی

سه سند در سی‌پی‌جی ارائه شده است:

۱. فهرست سی‌پی‌جی (که همین متن و سند نگاشته شده است).

۲. کاربرگ سی‌پی‌جی که در ادامه نمایش داده شده است.

۳. ماتریس کامل داده‌های سی‌پی‌جی که حاوی همه‌ی داده‌های خام سی‌پی‌جی‌ها، نگاشت و تنظیم آنها با چارچوب های دیگر و غیره است.

کاربرگ سی‌پی‌جی

علاوه بر فهرست سی‌پی‌جی‌ها، یک کاربرگ کاربرپسند برای سرمایه‌داران و اپراتورها وجود دارد که می‌توانند: الف) سی‌پی جی‌ها را بررسی و طبق نیاز اولویت‌بندی کنند. ب) امکان پیگیری وضعیت فعلی و آینده در صورت اجرای سی‌پی‌جی را داشته باشند. ج) اولویت‌ها، مبادلات و وضعیت سی‌پی‌جی‌ها را بدون ابهام به سرمایه‌گذاران و مدیران غیرفنی ابلاغ کنند.

کاربرگ شامل برآوردهای کلی هزینه، پیچیدگی و تاثیر دستیابی به هر هدف می‌شود. از این برآوردها باید به عنوان کمکی جهت اطلاع‌رسانی درباره رویه‌ی سرمایه‌گذاری برای شکاف‌های موجود در اساس امنیت سایبری بهره‌مند شد.

استفاده از کاربرگ سی‌پی‌جی

۱. یک خودارزیابی اولیه انجام شود. سازمان‌ها با بررسی برنامه‌های امنیتی موجود باید مشخص کنند که قبلا چه سی پی‌جی‌هایی اجرا شده‌اند. شاید سازمان‌ها از قبل دستورالعمل های مبتنی بر سی‌پی‌جی یا مقرراتی مانند NIST CSF یا ISA ۶۲۴۴۳ را پیاده کرده باشند.

۲. شکاف‌ها شناسایی و اولویت‌بندی شوند. سازمان‌ها با بررسی مشکلات و شکاف‌های موجود در نحوه‌ی اجراسازی سی پی‌جی، آنها را بر اساس هزینه، پیچیدگی و اثرگذاری اولویت بندی می‌کنند.

۳. سرمایه‌گذاری و اجرا. بعضی از سازمان‌ها ممکن است با کمک این کاربرگ بتوانند از بخش مدیریت جهت اختصاص بودجه برای پروژه‌های مربوط به امنیت سایبری درخواست کنند.

۴. میزان پیشرفت در هر ۱۲ ماه بررسی شود. برای این کار، سازمان‌ها پس از هر ۱۲ ماه کاربرگ را مجددا بررسی کنند تا بتوانند میزان پیشرفت را ارزیابی کنند. این موضوع هم به نفع مدیریت و هم به نفع اشخاص ثالث است.

امنیت حساب

1.1

تشخیص تلاش‌های ناموفق (خودکار) ورود به سیستم — **PR.AC-7**

پیامد

محافظت از سازمان‌ها در برابر حملات خودکار و هویتی

خطرات موردنظر یا تی‌تی‌پی (TTP)

Brute Force – Password Guessing (T1110.001)
Brute Force – Password Cracking (T1110.002)
Brute Force – Password Spraying (T1110.003)
Brute Force – Credential Stuffing (T1110.004)

محدوده

دارایی‌های فناوری اطلاعات و دارایی های جدید فناوری عملیاتی حفاظت شده با گذرواژه

اقدامات پیشنهادی

همه‌ی ورودهای ناموفق ثبت شده و به تیم امنیتی سازمان یا سیستم ثبت گزارش مربوطه ارسال می‌شود. تیم‌های امنیتی پس از تعداد مشخصی از تلاش‌های متوالی و ناموفق برای ورود به سیستم در یک دوره‌ی کوتاه (مثلا ۵ تلاش ناموفق در مدت ۲ دقیقه) مطلع می‌شوند (به عنوان مثال، با یک هشدار). این هشدار ثبت شده و در سیستم امنیتی برای تجزیه و تحلیل بیشتر ذخیره می‌شود.
برای دارایی‌های فناوری اطلاعات، یک سیاستی وجود دارد که از ورود حساب‌های مشکوک به سیستم جلوگیری می‌کند. برای مثال، حساب می‌تواند برای مدتی کوتاه یا تا زمانی که حساب توسط یک کاربر امتیازدار دوباره فعال شود، از دسترس خارج گردد. این پیکربندی زمانی فعال می‌شود که در یک دارایی موجود باشد. برای نمونه، ویندوز ۱۱ می‌تواند پس از ۱۰ بار تلاش ناموفق برای ورود در مدت ۱۰ دقیقه، به طور خودکار حساب‌ها را تا ۱۰ دقیقه قفل کند.

1.2

تغییر گذرواژه‌ی پیش‌فرض — PR.AC-1

پیامد

جلوگیری از استفاده‌ی سودجویان از گذرواژه‌های پیش‌فرض جهت دسترسی پیدا کردن و نفوذ به شبکه

خطرات موردنظر یا تی‌تی‌پی (TTP)

Valid Accounts – Default Accounts (T1078-001)
Valid Accounts (ICS T0859)

محدوده

دارایی‌های فناوری اطلاعات و دارایی های جدید فناوری عملیاتی حفاظت شده با گذرواژه

اقدامات پیشنهادی

سیاستی اجباری در سراسر سازمان که طبق آن گذرواژه‌های پیش‌فرض برای همه سخت‌افزار، نرم‌افزار و ثابت‌افزار قبل از قرار گرفتن در هر شبکه داخلی یا خارجی باید تغییر داده شود. این شامل دارایی‌های فناوری اطلاعات برای فناوری عملیاتی، مانند صفحات وب مدیریت فناوری عملیاتی می‌شود.

در مواردی که تغییر گذرواژه‌های پیش‌فرض امکان‌پذیر نیست (مانند یک سیستم کنترل با رمز عبور هاردکد)، نظارت های امنیتی لازم انجام شود و گزارش‌های ترافیک شبکه و تلاش‌های ورود به سیستم در آن دستگاه‌ها ثبت گردد.

فناوری عملیاتی: در حالی که تغییر گذرواژه‌های پیش‌فرض در اوتی (OT) موجود یک سازمان به نظر سخت می‌آید؛ اما همچنان توصیه می‌شود تا چنین سیاستی برای تغییر اطلاعات پیش‌فرض برای همه‌ی دستگاه‌های جدید در آینده اجرا شود. دستیابی به این امر نه تنها آسان‌تر است، بلکه در صورت تغییر تی‌تی‌پی‌های دشمن، خطر بالقوه را در آینده کاهش می‌دهد.

1.3

احراز هویت چندعاملی (MFA) **PR.AC-7**

پیامد

اضافه کردن یک لایه‌ی امنیتی قوی برای محافظت از دارایی حساب‌هایی که اطلاعات هویتی آنها دستکاری شده

خطرات موردنظر یا تی‌تی‌پی (TTP)

Brute Force (T1110)
Remote Services – Remote Desktop Protocol (T1021.001)
Remote Services – SSH (T1021.004)
Valid Accounts (T1078, ICS T0859)
External Remote Services (ICS T0822)

محدوده

دارایی‌هایآی‌تی و اوتی با دسترسی از راه دور مانند ورک استیشن‌ها و HMI در مواردی که ایمن و از نظر فنی توانا هستند.

اقدامات پیشنهادی

در صورت وجود، احراز هویت چندعاملی مبتنی بر سخت افزار فعال شود. در غیر این صورت، باید از سافت توکن (مثلا از طریق برنامه موبایلی) استفاده کرد. از احراز هویت چندعاملی از طریق پیامک فقط در صورتی که راه‌های دیگر امکان‌پذیر نباشند، می‌توان استفاده کرد.
آی‌تی: حساب‌های آی‌تی از MFA برای دسترسی به منابع سازمانی استفاده می‌کنند.
OT: در حوزه OT ، احراز هویت چندعاملی در همه حساب‌ها و سیستم‌هایی که می‌توان از راه دور به آن‌ها دسترسی پیدا کرد از جمله رابط‌های ماشین و انسان (HMI)، ورک استیشن‌های مهندسی و کاربری و حساب‌های مالی/تجارتی فعال است.

1.4

تعداد حداقلی کاراکتر برای داشتن گذرواژه قوی — PR.AC-1

پیامد

دشوارتر شدن حدس یا کشف گذرواژه‌های سازمانی

خطرات موردنظر یا تی‌تی‌پی (TTP)

Brute Force – Password Guessing (T1110.001)
Brute Force – Password Cracking (T1110.002)
Brute Force – Password Spraying (T1110.003)
Brute Force – Credential Stuffing (T1110.004)

محدوده

دارایی‌های آی‌تی و اوتی مبتنی بر ویندوز و محافظت شده با گذرواژه

اقدامات پیشنهادی

سیستم سازمان‌ها سیاستی را دنبال می‌کند که طبق آن حداقل تعداد کاراکتر گذرواژه‌ها برای دارایی‌های آی‌تی وآی‌تی محافظت‌شده با گذرواژه در صورت وجود امکانات فنی×، باید ۱۵×× یا بیشتر باشد. برای آسانتر شدن انتخاب و استفاده از گذرواژه‌های طولانی، سازمان‌ها باید به فکر برنامه‌های مدیریت‌کننده‌ی گذرواژه باشند. در مواردی که حداقل تعداد کاراکتر انتخابی برای گذرواژه از لحاظ فنی امکان‌پذیر نباشد، نظارت و کنترل‌های بیشتری اعمال و همه‌ی فعالیت‌ها و تلاش‌ها برای دسترسی به دارایی ثبت و گزارش شود. دارایی‌هایی که توان پشتیبانی از گذرواژه های قوی و طولانی را ندارند، باید جهت ارتقا یا جایگزینی در اولویت قرار بگیرند.

این مورد مخصوصا برای سازمان‌هایی که در آنها احراز هویت چندعاملی انجام نمی‌شود و توان مقابله با حملات بروت‌فورس (مانند فایروال‌های برنامه‌های وب و شبکه های انتقال محتوای شخص ثالث) را ندارند یا نمی‌توانند از روش‌های احراز هویت بدون نیاز به گذرواژه استفاده کنند، اهمیت دارد.

×ابزارهای مدرن به راحتی می‌توانند گذرواژه‌های ۸ کاراکتری را حدس بزنند. طولانی بودن گذرواژه مهم‌تر از پیچیدگی یا تغییر دادن مداوم آن است و از سوی دیگر، افراد می‌توانند به راحتی گذرواژه‌های طولانی را ایجاد کنند و بخاطر بسپرند.

××بیشتر دارایی‌های اوتی که از مکانیزم احراز هویت مرکزی (مانند اکتیو دایرکتوری) استفاده می‌کنند، مدنظر هستند. نمونه‌هایی از دارایی‌های اوتی که از لحاظ فنی توان کافی ندارند، عبارتند از آنهایی که در مکان‌های دورافتاده مانند دکل‌های دریایی یا بالای توربین‌های بادی قرار دارند.

1.5

جداسازی حساب‌های کاربری و امتیازدار — PR.AC-4

پیامد

دشوار کردن دسترسی مهاجمان به حساب‌های مهم و امتیازدار، حتی در صورت دستکاری شدن حساب‌های کاربری عادی

خطرات موردنظر یا تی‌تی‌پی (TTP)

Valid Accounts
(T1078, ICS T0859)

محدوده

دارایی‌های آی‌تی و اوتی ایمن، با قابلیت‌های فنی

اقدامات پیشنهادی

هیچ حساب کاربری عادی‌ای از قابلیت‌های فوق کاربری برخوردار نیست. ادمین‌ها از حساب‌های کاربری عادی برای انجام فعالیت‌های غیرمربوط به ادمینی مانند زدن ایمیل های تجاری یا گشتن در وب استفاده می‌کنند. امتیازهایی که به حساب‌های امتیازدار داده شده است، مکررا طی یک دوره‌ی خاص ارزیابی می‌شود.

1.6

اطلاعات منحصر به فرد	PR.AC-1

پیامد

پیشگیری از استفاده‌ی مجدد مهاجمان از اطلاعات هویتی دستکاری شده برای نفوذ به شبکه، به ویژه در شبکه‌های آی‌تی و اوتی

خطرات موردنظر یا تی‌تی‌پی (TTP)

Valid Accounts
(T1078, ICS T0859)
Brute Force – Password Guessing (T1110.001)

محدوده

دارایی‌های آی‌تی و اوتی

اقدامات پیشنهادی

سازمان‌ها برای خدمات مشابه و دسترسی به دارایی‌ها در شبکه‌های آی‌تی و اوتی، اطلاعات ورود منحصر به فرد و جداگانه‌ای ارائه می‌کنند. کاربران نمی‌توانند از گذرواژه های تکراری برای ورود به حساب، بهره‌مندی از برنامه‌ها و خدمات استفاده کنند.

1.7

لغو دسترسی کارکنان خارج شده از سازمان — PR.AC-1

پیامد	اقدامات پیشنهادی
ابطال دسترسی غیرمجاز کارکنان سابق به حساب‌ها یا منابع سازمانی	

خطرات موردنظر یا تی‌تی‌پی (TTP)	محدوده
Valid Accounts (T1078, ICS T0859)	کارکنان سابق

یک فرآیند تعریف‌شده و اجباری برای همه‌ی کارکنانی که قصد ترک سازمان را دارند، در روز خروجشان طی می شود: الف) همه‌ی کارت‌ها، کلیدها، توکن‌ها و دیگر وسایل فیزیکی سازمان بازگردانده می‌شود. ب) همه‌ی حساب‌های کاربری و راه‌های دسترسی آنها به منابع سازمانی غیرفعال می‌گردد.

امنیت دستگاه

2.1

فرآیند تایید سخت‌افزار و نرم‌افزار PR.IP-3

پیامد

افزایش آگاهی نسبت به شرایط فناوری‌های مورد استفاده و کاهش احتمال بروز مشکل با نصب نرم‌افزار، ثابت‌افزار و سخت‌افزار تأیید نشده از سوی کاربران

خطرات موردنظر یا تی‌تی‌پی (TTP)

Supply Chain Compromise (T1195, ICS T0862)
Hardware Additions (T1200)
Browser Extensions (T1176)
Transient Cyber Asset (ICS T0864)

محدوده

دارایی‌های آی‌تی و اوتی

اقدامات پیشنهادی

یک سیاست اداری یا فرآیند خودکار جهت استفاده از سخت‌افزار، ثابت‌افزار و نرم‌افزار تعریف می‌شود که نیاز به تأیید آنها پیش از نصب و اجرا دارد. سازمان‌ها یک فهرست از سخت‌افزار، نرم‌افزار و ثابت‌افزار تأیید شده با تهدیدات شناسایی‌شده نگهداری می‌کنند که اگر از لحاظ فنی امکان‌پذیر باشد، شامل مشخصات نسخه‌های جدید تأیید شده هم می‌شود. برای دارایی‌های اوتی، این اقدام باید همراه با فعالیت‌های مدیریت تغییر و تست باشد.

2.2

غیرفعال کردن ماکروها به طور دستی

PR.IP-3 ، PR.IP-1

پیامد	اقدامات پیشنهادی
کاهش متداول‌ترین و اثرگذارترین خطر ناشی از ماکرو های جاسازی شده و کدهای اجرایی مشابه	سیاستی که سیستم به طور پیش‌فرض همه‌ی ماکروهای آفیس مایکروسافت و کدهای تعبیه‌شده مشابه را غیرفعال می‌کند. اگر قرار باشد ماکروها در شرایط خاصی فعال شوند، فقط کاربران مجاز می‌توانند برای فعال شدن ماکروها در بعضی دارایی‌ها درخواست ثبت کنند.

خطرات موردنظر یا تی‌تی‌پی (TTP)	محدوده
Phishing – Spearphishing Attachment (T1566.001) User Execution – Malicious File (T1204.002)	دارایی‌های آی‌تی

2.3

موجودی دارایی	ID.AM-1

پیامد	اقدامات پیشنهادی
شناسایی دارایی‌های مهم، ناشناخته و مدیریت‌نشده برای تشخیص دادن هرچه سریع‌تر و پاسخگویی به آسیب پذیری‌های جدید	فهرستی از همه‌ی دارایی‌های سازمانی با آدرس آی‌پی (از جمله IPv۶) و مخصوصا اوتی تهیه شود. این فهرست باید مرتبا و حداقل در دوره‌های ماهانه برای آی‌تی و اوتی به روز شود.

خطرات موردنظر یا تی‌پی (TTP)	محدوده
Hardware Additions (T1200) Exploit Public-Facing Application (T0819, ICS T0819) Internet Accessible Device (ICS T0883)	دارایی‌های آی‌تی و اوتی

2.4

ممنوعیت اتصال دستگاه‌های تایید نشده و غیرمجاز — PR.PT-2

پیامد

جلوگیری از دسترسی مهاجمان سایبری به داده‌ها از طریق دستگاه‌های رسانه‌ای قابل حمل غیرمجاز

اقدامات پیشنهادی

سازمان‌ها برای اطمینان حاصل کردن از عدم اتصال ابزارها و سخت‌افزارهای غیرمجاز به دارایی‌های آی‌تی و اوتی، سیاست هایی از جمله محدودیت استفاده از یواس‌بی و غیرفعال سازی اجرای خودکار (AutoRun) را در پیش می‌گیرند.
اوتی: در صورت امکان، رویه‌هایی را برای حذف، غیرفعال سازی یا ایمن کردن پورت‌های فیزیکی جهت پیشگیری از اتصال دستگاه‌های غیرمجاز ایجاد شود. حتی می‌توان رویه هایی را برای اعطای دسترسی به موارد استثنا در صورت دریافت تأییدیه ایجاد کرد.

خطرات موردنظر یا تی‌تی‌پی (TTP)

Hardware Additions (T1200)
Replication Through Removable Media (T1091, ICS T0847)

محدوده

دارایی‌های آی‌تی و اوتی

2.5

ثبت پیکربندی دستگاه	PR.IP-1

پیامد	اقدامات پیشنهادی
پاسخگویی به حملات سایبری و بازیابی بعد از حمله، به روشی مؤثر و کارآمد	سازمان‌ها جزئیات اصلی و پیکربندی فعلی همه دارایی های مهم آی‌تی و اوتی را ثبت می‌کنند تا مدیریت آسیب پذیری‌ها، پاسخگویی به حملات سایبری و بازیابی بعد از انجام حمله به بهترین شکل ممکن انجام شود. بررسی‌ها و به روزرسانی‌های دوره‌ای مرتبا انجام می‌شود.

خطرات موردنظر یا تی‌تی‌پی (TTP)	محدوده
ناکافی یا ناقص بودن توان بازیابی عملکرد دستگاه‌های حیاتی و اپراتور های خدمات‌رسان، یا حتی تأخیر در اقدام	دارایی‌های آی‌تی و اوتی

امنیت داده

3.1

مجموعه گزارش (لاگ) — **PR.PT-1**

پیامد

افزایش توان شناسایی و پاسخگویی بهتر به حملات سایبری

خطرات موردنظر یا تی‌تی‌پی (TTP)

ناکافی یا ناقص بودن توان شناسایی و پاسخگویی به حوادث احتمالی سایبری، یا حتی تأخیر در اقدام

خطوط دفاعی ضعیف (T1562)

محدوده

دارایی‌های آی‌تی و اوتی

اقدامات پیشنهادی

از گزارش‌های دسترسی و امنیت جمع‌آوری و ذخیره شده (برای مثال IDS/IDPS، فایروال، VPN و DLP) در شناسایی و پاسخگویی به حملات سایبری (مانند پزشکی قانونی) استفاده می‌شود. تیم‌های امنیتی به محض غیرفعال شدن منابع مهم گزارش مانند ثبت رویدادهای ویندوزی، مطلع می‌شوند.

اوتی: در دارایی‌های اوتی که گزارش‌ها غیراستاندارد یا غیرقابل دسترسی هستند، میزان ترافیک شبکه و اتصالات به دارایی‌های بدون قابلیت ثبت گزارش، بررسی و ذخیره می‌شود.

3.2

ذخیره‌سازی ایمن گزارش‌ها — PR.PT-1

پیامد

حفاظت از گزارش‌های امنیتی سازمان‌ها در برابر دسترسی های غیرمجاز و دستکاری شدن

خطرات موردنظر یا تی‌تی‌پی (TTP)

Indicator Removal on Host - Clear Windows Event Logs (T1070.001)
Indicator Removal on Host - Clear Linux or Mac System Logs (T1070.002)
Indicator Removal on Host - File Deletion (T1070.004)
Indicator Removal on Host (ICS T0872)

محدوده

دارایی‌های آی‌تی و اوتی

اقدامات پیشنهادی

گزارش‌ها در یک سیستم مرکزی مانند ابزار اطلاعات امنیتی و مدیریت رویداد (SIEM) یا در پایگاه داده مرکزی ذخیره می‌شوند و فقط کاربران مجاز و تأییدشده می توانند به آنها دسترسی پیدا کنند. این گزارش‌ها به مدت زمان تعیین شده در دستورالعمل‌های نظارتی ذخیره می شوند.

3.3

رمزگذاری قوی و سریع	PR.DS-2 ، PR.DS-1

پیامد

رمزگذاری مؤثر برای حفظ محرمانگی داده‌های حساس و یکپارچگی ترافیک آی‌تی و اوتی

خطرات موردنظر یا تی‌تی‌پی (TTP)

Adversary-in-the-Middle (T1557)
Automated Collection (T1119)
Network Sniffing (T1040, ICS T0842)
Wireless Compromise (ICS T0860)
Wireness Sniffing (ICS T0887)

محدوده

ترافیک همه دارایی های آی‌تی و دارایی های از راه دور اوتی (آن‌هایی که در ارتباط با نهادهای خارجی هستند)

اقدامات پیشنهادی

از امینت لایه انتقال (TLS) پیکربندی و به‌روز شده برای محافظت از داده‌ها در حین انتقال در جاهایی که از نظر فنی امکان‌پذیر هستند، استفاده می‌شود. سازمان‌ها باید برای شناسایی هرگونه استفاده از رمزگذاری قدیمی یا ضعیف و به روزرسانی الگوریتم‌ها برنامه‌ریزی کنند و برای مدیریت پیامدهای رمزنگاری پس کوانتومی توان کافی داشته باشند.

اوتی: از رمزگذاری (در جاهایی که از لحاظ فنی امکان‌پذیر باشد) معمولا برای کاهش میزان دسترسی در ارتباطات اوتی با دارایی‌های خارجی و از راه دور استفاده می‌شود.

3.4

محافظت از داده‌های حساس | **PR.DS-1، PR.DS-2، PR.DS-5**

پیامد

محافظت از اطلاعات حساس در برابر دسترسی غیرمجاز

خطرات موردنظر یا تی‌تی‌پی (TTP)

اطلاعات هویتی ناامن (T1552)

سرقت یا جعل مجوز کربروس (T1558)

دامپینگ اطلاعات سیستم عامل (T1003)

داده‌های مخازن اطلاعات (ICS T0811)

سرقت اطلاعات عملیاتی (T0882)

محدوده

همه‌ی گذرواژه‌ها، اطلاعات هویتی، اسرار و سایر اطلاعات حساس یا کنترل‌شده

اقدامات پیشنهادی

داده‌های حساس که شامل اطلاعات هویتی می‌شود، در هیچ جا به صورت متنی ذخیره نمی‌شود و فقط کاربران مجاز و تأییدشده می‌توانند به آن دسترسی پیدا کنند. اطلاعات هویتی به شکلی ایمن و با مدیریت‌کننده‌های گذرواژه یا دیگر راه حل‌های مدیریت حساب‌های امتیازدار، ذخیره می‌شود.

نحوه‌ی اداره کردن و آموزش

4.1

رهبری امنیت سایبری سازمانی	ID.GV-1، ID.GV-2

پیامد

یک رهبر مسئولیت امنیت سایبری در یک سازمان را بر عهده دارد

خطرات موردنظر یا تی‌تی‌پی (TTP)

نبود مسئولیت‌پذیری، پاسخگویی، سرمایه‌گذاری یا اثربخشی کافی در زمینه امنیت سایبری

محدوده

-

اقدامات پیشنهادی

یک نقش به عنوان مسئول و پاسخگو برای برنامه‌ریزی، تأمین منبع و اجرای فعالیت‌های امنیت سایبری تعریف می شود. فعالیت‌هایی از جمله مدیریت امنیت سایبری در سطوح بالا، درخواست و تأمین منبع بودجه یا رهبری استراتژی توسعه برای جهت‌گیری در آینده، در محدوده‌ی فعالیت و رهبری این نقش قرار دارد.

4.2

رهبری امنیت سایبری اوتی	ID.GV-1، ID.GV-2

پیامد

یک رهبر مسئولیت پاسخگویی به موارد مربوط به امنیت سایبری در زمینه‌ی اوتی و دارایی‌های اوتی در یک سازمان را بر عهده دارد.

اقدامات پیشنهادی

یک نقش به عنوان مسئول و پاسخگو برای برنامه‌ریزی، تأمین منبع و اجرای فعالیت‌های مرتبط با امنیت سایبری در زمینه اوتی تعریف می‌شود.

خطرات موردنظر یا تی‌تی‌پی (TTP)

نبود مسئولیت‌پذیری و پاسخگویی، سرمایه‌گذاری یا اثربخشی در برنامه امنیت سایبری OT

محدوده

-

4.3

آموزش مقدماتی امنیت سایبری	PR.AT-1

پیامد

به کارکنان سازمانی آموزش داده می‌شود تا رفتارهای درست و ایمن از خود نشان دهند

اقدامات پیشنهادی

باید آموزش‌های مربوط به مفاهیم اساسی امنیتی مانند فیشینگ، دستکاری ایمیل تجاری، امنیت عملیات مقدماتی (OPSEC)، امنیت گذرواژه و تقویت فرهنگ امنیت سایبری و آگاهی داخلی، حداقل به صورت سالانه به کارکنان سازمانی و پیمانکاران داده شود. کارکنان جدید در ده روز اول شروع به کار، آموزش‌های مقدماتی امنیت سایبری به آن‌ها ارائه می‌شود و حداقل این آموزش ها به صورت سالیانه مرور می‌گردد.

خطرات موردنظر یا تی‌تی‌پی (TTP)

User Training
(M1017, ICS M0917)

محدوده

همه‌ی کارکنان و پیمانکاران

4.4

آموزش امنیت سایبری OT	PR.AT-2، PR.AT-3، PR.AT-5

پیامد	اقدامات پیشنهادی
کارکنان بخش امنیت دارایی‌های OT، آموزش‌های تخصصی در زمینه OT دریافت می‌کنند	علاوه بر آموزش‌های مقدماتی امنیت سایبری، آموزش‌های تخصصی امنیت سایبری در زمینه OT سالیانه به کارکنانی که وظیفه حفظ و تأمین ایمنی دارایی‌های OT را دارند داده می‌شود.

خطرات موردنظر یا تی‌تی‌پی (TTP)	محدوده
User Training (M1017, ICS M0917)	همه کارکنان بخش امنیت OT

4.5

بهبود روابط امنیت سایبری IT و OT | **ID.GV-2**

پیامد

بهبود امنیت سایبری اوتی و تسریع پاسخگویی مؤثر به حوادث سایبری اوتی

خطرات موردنظر یا تی‌تی‌پی (TTP)

روابط کاری ضعیف و نبود درک متقابل بین امنیت سایبری آی‌تی و اوتی اغلب می‌تواند منجر به افزایش خطرات و تهدیدات برای امنیت سایبری در زمینه‌ی اوتی شود.

محدوده

همه‌ی کارکنان بخش امنیت آی‌تی و اوتی

اقدامات پیشنهادی

سازمان‌ها سالیانه حداقل یکبار گردهمایی تشکیل می دهند تا روابط کاری بین کارکنان بخش‌های امنیتی آی‌تی و اوتی تقویت شود. البته این نوع گردهمایی یک رویداد کاری نیست.

مدیریت آسیب‌پذیری

5.1

کاهش آسیب‌پذیری‌های شناخته شده | **PR.IP-12، ID.RA-1، DE.CM-8، RS.MI-3**

پیامد

کاهش احتمال سوءاستفاده‌ی مهاجمان از آسیب‌پذیری های شناخته شده برای نفوذ به شبکه‌های سازمانی

خطرات موردنظر یا تی‌تی‌پی (TTP)

Active Scanning - Vulnerability Scanning (T1595.002)
Exploit Public-Facing Application (T1190, ICS T0819)
Exploitation of Remote Service (T1210, ICS T0866)
Supply Chain Compromise (T1195, ICS T0862)
External Remote Services (T1133, ICS T0822)

محدوده

دارایی‌های متصل به اینترنت

اقدامات پیشنهادی

همه‌ی آسیب‌پذیری‌های شناخته شده (موجود در فهرست KEV ارائه شده از سوی CISA به نشانی https://www.cisa.gov/known-exploited-vulnerabilities-catalog) در سیستم‌های متصل به اینترنت به ویژه دارایی‌های مهم و اولویت‌دار پَچ شده یا اثر خطرات ناشی از آنها در مدت زمان مشخص به حداقل رسانده شده است.
اوتی: برای دارایی‌هایی که قابل پچ کردن نیستند یا امکان کاهش میزان دسترسی و امنیت آنها وجود دارد، اقدام‌های جبران‌کننده (مانند دسته‌بندی و نظارت) اعمال و ثبت می‌شود. اقدام‌های کنترل‌کننده باعث غیرقابل دسترس شدن دارایی‌ها از طریق اینترنت عمومی می‌شود یا توان مهاجمان برای سوءاستفاده از آسیب‌پذیری‌های موجود در این دارایی‌ها را کاهش می‌دهد.

5.2

اعلام یا افشای آسیب‌پذیری — **RS.AN-5**

پیامد

آسیب‌پذیری‌ها و نقاط ضعف موجود در دارایی‌ها سریع‌تر از سوی محققان امنیتی سازمان‌ها شناسایی می‌شوند. آنها یافته‌های خود را به اشتراک می‌گذارند.

خطرات موردنظر یا تی‌تی‌پی (TTP)

Active Scanning - Vulnerability Scanning (T1595.002)
Exploit Public-Facing Application (T1190, ICS T0819)
Exploitation of Remote Service (T1210, ICS T0866)
Supply Chain Compromise (T1195, ICS T0862)

محدوده

همه دارایی‌ها

اقدامات پیشنهادی

مطابق با NIST SP ۸۰۰-۵۳ Revision ۵ ، سازمان‌ها روشی عمومی و راحت به محققان ارائه می‌دهند تا به تیم امنیتی سازمان درباره‌ی آسیب‌پذیری‌ها، دارایی‌های که اشتباه پیکربندی شده‌اند یا دیگر موارد مشکوک اطلاع دهند. موارد قابل تامل بررسی می‌شوند و به آنها پاسخ مناسب در مدت زمان مشخص داده می‌شود. به نقاط ضعف نام برده شده هم طبق سطح پیچیدگی و خطراتی که به همراه دارند، رسیدگی می‌شود.

محققان امنیتی‌ای که آسیب‌پذیری‌های شناسایی شده را به اشتراک می‌گذارند، تحت قوانین سیف هاربر (Safe Harbor) محافظت می‌شوند. در مواردی که آسیب‌پذیری ها تأیید و رسیدگی شوند، از محققی که آن را شناسایی و اطلاع‌رسانی کرده است، قدردانی می‌گردد.

5.3

استقرار فایل‌های Security.txt — RS.AN-5

پیامد

به محققان امنیتی اجازه‌ی ثبت و گزارش سریع‌تر نقاط ضعف و آسیب‌پذیری‌های شناسایی شده را می‌دهد.

خطرات موردنظر یا تی‌تی‌پی (TTP)

Active Scanning - Vulnerability Scanning (T1595.002)
Exploit Public-Facing Application (T1190, ICS T0819)
Exploitation of Remote Service (T1210, ICS T0866)
Supply Chain Compromise (T1195, ICS T0862)

محدوده

همه‌ی دامنه‌های وب در دسترس برای عموم

اقدامات پیشنهادی

همه‌ی دامنه‌های وب عمومی دارای یک فایل .Secutiry txt هستند که مطابق با توصیه‌های RFC ۹۱۱۶ هستند.

5.4

محدود کردن سوءاستفاده‌گری در اینترنت — PR.PT-4

پیامد

کاربران غیرمجاز نمی‌توانند با بهره‌برداری از ضعف‌های شناخته شده در دارایی‌های عمومی، امکان دسترسی اولیه به سیستم را به دست آورند.

خطرات موردنظر یا تی‌تی‌پی (TTP)

Active Scanning - Vulnerability Scanning (T1595.002)
Exploit Public-Facing Application (T1190, ICS T0819)
Exploitation of Remote Service (T1210, ICS T0866)
External Remote Services (T1133, ICS T0822)
Remote Services - Remote Desktop Protocol (T1021.001)

محدوده

دارایی‌های آی‌تی و اوتی در اینترنت عمومی

اقدامات پیشنهادی

دارایی‌های موجود در اینترنت عمومی هیچ خدمات قابل بهره‌برداری مانند RDP را در معرض دید قرار نمی‌دهند. در مواردی که این خدمات باید در معرض دید قرار گیرند، اقدامات جبرانی و کنترل‌های مناسب برای جلوگیری از اشکال رایج سوءاستفاده و بهره‌برداری اعمال می‌شود. همه‌ی برنامه‌های غیرضروری سیستم عامل و پروتکل های شبکه در دارایی‌های مرتبط با اینترنت غیرفعال هستند.

5.5

محدود کردن اتصالات اوتی به اینترنت PR.PT-4

پیامد

کاهش خطرات مربوط به سوءاستفاده یا اخلال در دارایی های اوتی متصل به اینترنت عمومی

خطرات موردنظر یا تی‌تی‌پی (TTP)

Active Scanning - Vulnerability Scanning (T1595.002)
Exploit Public-Facing Application (T1190, ICS T0819)
Exploitation of Remote Service (T1210, ICS T0866)
External Remote Services (T1133, ICS T0822)

محدوده

دارایی‌های اوتی در اینترنت عمومی

اقدامات پیشنهادی

هیچ دارایی اوتی در اینترنت عمومی قرار نگیرد، مگر دارایی‌هایی که برای ادامه‌ی فعالیتشان به آن وابسته هستند. استثناها باید توجیه شده و مستند شوند و دارایی های استثنا شده باید لایه‌های حفاظتی اضافی برای شناسایی و جلوگیری از تلاش‌ها برای سوءاستفاده‌گری (مانند ورود به سیستم، MFA، دسترسی اجباری از طریق پروکسی یا سایر واسطه‌ها) داشته باشند.

5.6

اعتبارسنجی اثربخشی کنترل امنیت سایبری توسط شخص ثالث — ID.RA-1، ID.RA-3

پیامد

شناسایی استراتژی‌ها و تکنیک‌های امنیتی که فاقد لایه دفاعی مناسب هستند.

خطرات موردنظر یا تی‌تی‌پی (TTP)

کاهش خطر ناشی از وجود شکاف در خطوط دفاعی سایبری

محدوده

دارایی‌ها و شبکه های آی‌تی و اوتی

اقدامات پیشنهادی

اشخاص ثالث با تخصص خود در امنیت سایبری (آی‌تی و/یا اوتی) به طور منظم میزان اثربخشی و پوشش دفاعی امنیت سایبری سازمان را بررسی و تأیید می‌کنند. این تلاش ها که ممکن است شامل تست‌های نفوذ ، باگ باونتی (bug bounty)، شبیه‌سازی حادثه یا تمرین‌های table-top باشد، باید شامل تست‌های از پیش اعلام‌نشده و اعلام شده باشد.

تمرین‌ها هم توانایی و تأثیر یک مهاجم بالقوه برای نفوذ به شبکه از بیرون را در نظر می‌گیرد و هم توانایی یک مهاجم در داخل شبکه (به عنوان مثال، "فرض کردن نقض") را همراه با نشان دادن تأثیر بالقوه بر سیستم‌های حیاتی (از جمله OT/ICS)

مواردی که منجر به یافته‌های کاربردی و مؤثر باشد، دیگر در تمرین‌های بعدی مطرح نمی‌شود.

زنجیره‌ی تامین/شخص ثالث

6.1

الزامات امنیت سایبری برای فروشنده/تأمین‌کننده | **ID.SC-3**

پیامد

خرید محصولات و خدمات از تأمین‌کنندگان ایمن جهت کاهش خطر

خطرات موردنظر یا تی‌تی‌پی (TTP)

Supply Chain Compromise (T1195, ICS T0862)

محدوده

تأمین‌کنندگان دارایی و خدمات آی تی و اوتی

اقدامات پیشنهادی

اسناد تدارکاتی سازمان‌ها شامل الزامات و سؤالات امنیت سایبری برای فروشندگان است که از بین پیشنهادات با هزینه و عملکرد تقریبا مشابه، آن پیشنهادی که ایمن‌تر است، ترجیح داده می‌شود.

6.2

اعلام رخداد در زنجیره تأمین | **ID.SC-1، ID.SC-3**

پیامد

سازمان‌ها سریعتر از حوادث یا نقض‌های شناخته شده برای فروشندگان و ارائه‌دهندگان خدمات، مطلع می‌شوند و به آها پاسخ می‌دهند.

خطرات موردنظر یا تی‌تی‌پی (TTP)

Supply Chain Compromise
(T1195, ICS T0862)

محدوده

تأمین‌کنندگان دارایی و خدمات آی تی و اوتی

اقدامات پیشنهادی

اسناد و قراردادهای تدارکات، مانند قراردادهای سطح خدمات (SLAs)، تصریح می‌کنند که فروشندگان و/یا ارائه‌دهندگان خدمات باید مشتری را از خطر حوادث امنیتی در یک بازه زمانی تعیین‌شده از سوی سازمان‌ها مطلع کنند.

6.3

افشای آسیب‌پذیری در زنجیره تأمین — ID.SC-1، ID.SC-3

پیامد

سازمان‌ها سریع‌تر درباره آسیب‌پذیری‌های دارایی‌های ارائه شده توسط فروشندگان و ارائه‌دهندگان خدمات مطلع می‌شوند و به آنها پاسخ می‌دهند.

خطرات موردنظر یا تی‌تی‌پی (TTP)

Supply Chain Compromise (T1195، ICS T0862)

محدوده

تأمین‌کنندگان دارایی و خدمات آی تی و او تی

اقدامات پیشنهادی

اسناد و قراردادهای تدارکات، مانند قراردادهای سطح خدمات (SLAs)، تصریح می‌کنند که فروشندگان و/یا ارائه‌دهندگان خدمات، باید مشتری را از آسیب‌پذیری‌های امنیتی تأیید شده در یک بازه زمانی تعیین شده از سوی سازمان‌ها مطلع کنند.

پاسخگویی و بازیابی

7.1

گزارش حادثه | **RS.CO-2، RS.CO-4**

پیامد

CISA و سازمان‌های دیگر بهتر می‌توانند جهت رسیدگی به حملات سایبری یا درک بهتر آنها کمک کنند.

خطرات موردنظر یا تی‌تی‌پی (TTP)

بدون گزارش به موقع حادثه، CISA و سایر گروه‌ها کمتر قادر به کمک به سازمان‌های آسیب‌دیده هستند و به اطلاعات حیاتی کافی درباره گستردگی تهدید دست نمی‌یابند (مانند این که آیا حمله گسترده‌تری علیه یک بخش خاص رخ می‌دهد یا خیر).

محدوده

در سطح سازمانی

اقدامات پیشنهادی

سازمان‌ها سیاست‌ها و رویه‌هایی را در مورد این که چه کسی و چگونه همه‌ی حوادث امنیتی سایبری تأیید شده را به نهادهای خارجی مناسب گزارش کند (مانند تنظیم کننده‌های ایالتی/فدرال یا SRMA در صورت لزوم، ISAC/ISAO، و همچنین CISA)، دنبال می‌کنند. حوادث شناخته شده به CISA و همچنین سایر طرف‌های ضروری در بازه‌های زمانی تعیین شده، خواه طبق راهنما های نظارتی قابل اجرا و خواه در نبود راهنما، فورا گزارش می‌شوند. این هدف پس از اجرای کامل قانون گزارش دهی حوادث سایبری برای زیرساخت‌های حیاتی سال ۲۰۲۲ (CIRCIA) مورد بازنگری قرار خواهد گرفت.

7.2

طرح‌های واکنش به حادثه (IR)

PR.IP-9، PR.IP-10

پیامد

سازمان‌ها طرح‌های واکنش به حوادث امنیت سایبری را برای سناریوهای تهدید مربوطه حفظ، تمرین و به روزرسانی می‌کنند.

خطرات موردنظر یا تی‌تی‌پی (TTP)

ناتوانی در مهار سریع و مؤثر و کاهش برقراری ارتباط در حوادث امنیت سایبری

محدوده

در سطح سازمانی

اقدامات پیشنهادی

سازمان‌ها تکنیک‌ها و طرح‌های پاسخگویی به حوادث امنیت سایبری مربوط به آی‌تی و اوتی را برای سناریوهای تهدید معمول و مختص به سازمان (مثلا بر اساس بخش، محل، و غیره) را حفظ، به‌روزرسانی و به طور منظم تمرین می‌کنند. زمانی که آزمایش‌ها یا تمرین‌ها انجام می شوند، تا حد ممکن طبق شرایط واقعی شبیه‌سازی می شوند. طرح‌های IR حداقل سالیانه بازنگری و تمرین می شوند. سپس در یک بازه زمانی بعد از تمرین، طبق یافته‌ها به روز می‌گردند.

7.3

پشتیبان‌گیری از سیستم — PR.IP-4

پیامد

کاهش احتمال از دست دادن داده‌ها و تأخیر در ارائه خدمات یا انجام عملیات

خطرات موردنظر یا تی‌تی‌پی (TTP)

Data Destruction (T1485, ICS T0809)
Data Encrypted for Impact (T1486)
Disk Wipe (T1561)
Inhibit System Recovery (T1490)
Denial of Control (ICS T0813)
Denial/Loss of View (ICS T0815, T0829)
Loss of Availability (T0826)
Loss/Manipulation of Control (T0828, T0831)

محدوده

دارایی‌های آی‌تی و اوتی لازم برای عملیات تجاری

اقدامات پیشنهادی

تمام سیستم‌هایی که در عملیات ضروری هستند، به طور منظم و حداقل یک بار در سال، پشتیبان‌گیری می‌شوند. پشتیبان‌گیری‌ها جدا از سیستم‌های منبع ذخیره می شوند و به صورت مکرر، حداقل یک بار در سال آزمایش می‌شوند. اطلاعات ذخیره شده برای دارایی‌های اوتی حداقل شامل: پیکربندی‌ها، نقش‌ها، کنترلگر منطقی برنامه‌پذیر (PLC logic)، نقشه‌های مهندسی و ابزار است.

7.4

توپولوژی شبکه اسناد	PR.IP-1

پیامد	اقدامات پیشنهادی
پاسخگویی کارآمدتر و مؤثرتر به حملات سایبری و حفظ تداوم ارائه خدمات	سازمان‌ها اسناد دقیقی و به روز شده‌ای از توپولوژی شبکه و اطلاعات مربوطه در تمام شبکه‌های آی‌تی و اوتی دارند. بررسی‌ها و به‌روزرسانی‌های دوره‌ای باید به صورت مکرر انجام و پیگیری شوند.

خطرات مورد نظر یا تی‌تی‌پی (TTP)	محدوده
درک ناقص یا نادرست از توپولوژی شبکه مانع از نشان دادن واکنش مؤثر به حادثه و بازیابی پس از آن می شود.	همه‌ی شبکه‌های آی‌تی و اوتی

سایر

8.1

تقسیم‌بندی شبکه — **PR.AC-5، PR.PT-4، DE.CM-1**

پیامد

کاهش احتمال دسترسی مهاجمان به شبکه‌ی اوتیبعد از دستکاری شبکه‌ی آی‌تی

خطرات موردنظر یا تی‌تی‌پی (TTP)

Network Service Discovery (T1046)

Trusted Relationship (T1199)

Network Connection Enumeration (ICS T0840)

Network Sniffing (T1040، ICS T0842)

محدوده

دارایی‌های آی‌تی و اوتی، در جاهایی که ایمن و از نظر فنی توانا هستند.

اقدامات پیشنهادی

همه‌ی اتصالات به شبکه‌ی اوتی به طور پیش‌فرض ممنوع می‌شوند؛ مگر این که برای عملکرد سیستم خاصی مستقیما مجوز داده شود (به عنوان مثال توسط نشانی آی پی و پورت). مسیرهای ارتباطی لازم بین شبکه‌های آی‌تی و اوتی باید از طریق یک واسطه مانند فایروال پیکربندی شده، میزبان سنگر (bastion host)، jump box یا یک منطقه‌ی غیرنظامی (DMZ) میسر شود. واسطه‌هایی که به دقت نظارت می‌شوند، گزارش‌های شبکه را ضبط می کنند و فقط دارایی‌های تأیید شده‌ی مجاز می‌توانند به آنها وصل شوند.

8.2

شناسایی تهدیدات و TTPهای مرتبط

ID.RA-3, DE.CM-1

پیامد

سازمان‌ها از تهدیدها و تیتی‌پی‌های مرتبط آگاه و قادر به شناسایی آنها هستند.

خطرات موردنظر یا تی‌تی‌پی (TTP)

نداشتن اطلاعات درباره‌ی تهدیدات و ناتوانی در شناسایی آنها، باعث می شود تا سازمان‌ها مهاجمانی را که در شبکه‌های خود برای مدت طولانی حضور داشته و دارند، شناسایی نشده رها کنند.

محدوده

-

اقدامات پیشنهادی

سازمان‌ها فهرستی از تهدیدات و روش‌های مهاجمان برای نفوذ به سیستم‌های خود تهیه می‌کنند (مانند فهرست هایی که براساس صنعت، بخش و غیره تقسیم‌بندی شده اند) و این توانایی را دارند که از طریق قوانین، هشدارها یا سیستم‌های شناسایی و پیشگیری، نمونه‌هایی از آن تهدیدات را شناسایی کنند.

8.3

امنیت ایمیل | **PR.DS-1، PR.DS-2، PR.DS-5**

پیامد

کاهش خطرات ناشی از تهدیدات معمول مبتنی بر ایمیل، از جمله اسپوفینگ، فیشینگ و جاسوسی

خطرات موردنظر یا تی‌تی‌پی (TTP)

Phishing(T1566)

دستکاری ایمیل تجاری

محدوده

زیرساخت همه ایمیل‌های سازمانی

اقدامات پیشنهادی

در همه‌ی زیرساخت‌های ایمیل شرکتی الف) STARTTLS فعال است، ب) SPF و DKIM فعال است و ج) DMARC فعال و روی حالت «رد» تنظیم شده است. برای دیدن مثال ها و اطلاعات بیشتر به راهنمای CISA به نشانی https://www.cisa.gov/binding-operational-directive-18-01 مراجعه کنید.

فهرست معانی

فهرست کنترل دسترسی (ACL): فهرستی از سیستم‌های مجاز برای دسترسی به منابع

مدیریت دامنه: مجموعه‌ای از هاست‌ها و شبکه‌ها (مانند بخش، ساختمان، شرکت، سازمان) که تحت سیاست های مشترکی اداره می‌شود.

دارایی: به شخص، ساختار، تسهیلات، اطلاعات، وسیله یا هر فرآیند ارزشمندی گفته می‌شود.

قفل خودکار حساب کاربری یا تعیین حد مجاز برای ورود به حساب: سیاستی که تعداد تلاش‌های ناموفق برای ورود به سیستم را تعیین و نهایتا باعث قفل شدن حساب کاربری می‌شود.

پیکربندی پایه: مجموعه‌ی مستندی است از مشخصات یک سیستم اطلاعاتی یا یک آیتم پیکربندی در داخل یک سیستم که رسما مورد بررسی و تأیید قرار گرفته و تغییر دادن آن فقط از راه تغییر رویه‌های نظارتی امکان‌پذیر است.

ارزیابی تأثیر کسب و کار یا تجزیه و تحلیل تأثیر کسب و کار: به معنی تجزیه و تحلیل نیازمندی‌ها، عملکرد و وابستگی‌های یک سیستم اطلاعاتی است که الزامات و اولویت‌های آن سیستم را در صورت بروز اختلال احتمالی مشخص می‌کند.

مدیریت تحول: ایجاد تغییر و تحول برای پیشرفت سازمانی. رویکردی که طی آن، وضعیت فعلی سازمان برای دستیابی به مزایا و اهداف موردنظر تغییر پیدا می‌کند.

پیکربندی: شرایط، پارامترها و مشخصات احتمالی‌ای که یک سیستم اطلاعاتی یا بخشی از یک سیستم را توصیف یا طبقه‌بندی می‌کند.

نظارت مستمر: تحت نظر داشتن شرایط و آگاهی یافتن از خطرات احتمالی.

آسیب‌پذیری‌ها و تهدیدات رایج (CVE): فهرستی از نامگذاری‌ها و اصطلاحات مربوط به مشکلات نرم‌افزاری در حوزه‌ی امنیت.

کنترل‌های جبران‌کننده: تنظیمات امنیتی و حریم خصوصی، آن‌طور که در NIST Special Publication ۸۰۰-۵۳ شرح داده شده است، که برای حفاظت از یک سیستم یا سازمان ارائه می‌شود.

سیستم‌های نظارتی: سیستمی که جهت دستیابی به تغییر موردنظر در یک متغیر، عمدا دستکاری می‌شود. سیستم‌های نظارتی شامل PLC، DCS، SCADA و انواعی از سیستم‌های اندازه‌گیری و نظارتی صنعتی است.

تعلیم آگاهی امنیت سایبری یا برنامه‌ی آموزشی آگاهی از امنیت فناوری اطلاعات: قوانین رفتاری مناسب برای استفاده از سیستم‌های اطلاعاتی سازمان را توضیح می دهد. این برنامه خط مشی‌ها و رویه‌های امنیتی فناوری اطلاعات (IT) را که باید دنبال شوند، به اشتراک می‌گذارد.

چرخه‌ی حیات امنیت سایبری: موفقیت سرویس‌های فدرالی در ماموریت‌های حیاتی، به سیستم‌های اطلاعاتی وابسته است. به همین دلیل و با توجه به پیچیدگی روزافزون سیستم‌های اطلاعاتی و تهدیدات محیطی، امنیت اطلاعات به موضوع مهمی تبدیل شده است. هدف از تأمین امنیت اطلاعات این است که خطرات مربوط به اطلاعات سپرده شده به یک سرویس کاهش یابد تا در جهت خدمت به مردم مفید واقع شود. اگر از امنیت اطلاعات به صورت صحیح و مؤثر و در جهت حفظ محرمانگی، یکپارچگی و افزایش میزان دسترسی اطلاعات استفاده شود، می‌تواند به عاملی برای کسب و کار مبدل گردد.

طرح پاسخگویی به حوادث امنیت سایبری یا طرح رویارویی با پیشامد: مجموعه‌ای از دستورالعمل‌ها یا رویه های از پیش تعیین شده برای شناسایی، محدود کردن و پاسخگویی به پیامدهای ناشی از حملات سایبری مخرب علیه سیستم(های) اطلاعاتی یک سازمان.

گذرواژه‌ی پیش‌فرض: تنظیمات نرم‌افزار پیش‌فرض کارخانه در سیستم‌ها، دستگاه‌ها و وسایل تعبیه شده اغلب دارای گذرواژه‌های ساده‌ای است که برای همه‌ی سیستم‌ها در یک خط تولید مشترک است. از گذرواژه‌های پیش‌فرض در آزمایش‌های اولیه، نصب و پیکربندی استفاده می‌شود و توصیه‌ی بسیاری از فروشندگان این است که پیش از به کار گرفتن سیستم، گذرواژه‌ی پیش‌فرض تغییر داده شود.

منطقه‌ی غیرنظامی (DMZ): شبکه‌ای (واسطی) که بین شبکه‌های داخلی و خارجی قرار دارد. نقش آن، اجرای سیاست تضمین اطلاعات شبکه داخلی برای تبادل با اطلاعات خارجی و حفاظت از اطلاعات داخلی در برابر حملات خارجی با محدود کردن دسترسی به اطلاعات قابل انتشار است.

رمزگذاری (Encrypt): تبدیل داده‌ها به متون رمزی.

رمزگذاری (Encryption): به هر نوع روش تبدیل متن ساده به متن رمزی گویند که برای کسی جز گیرنده خوانا نباشد.

فایل اجراپذیر: انجام وظایف مشخص شده طبق دستورالعمل‌های کدگذاری شده با استفاده از یک برنامه یا روال رایانه‌ای.

فایروال یا سپرواره: دستگاه اتصال بین شبکه‌ای که ترافیک ارتباط داده بین دو شبکه متصل را محدود می‌کند. فایروال می‌تواند یک برنامه‌ی نصب شده در رایانه یا یک پلتفرم اختصاصی باشد که داده‌ها را در یک شبکه انتقال می دهد. معمولاً فایروال‌ها تعیین‌کننده‌ی مرز فعالیت هستند و به طور کلی قوانینی برای محدود کردن پورت‌های باز دارند.

ثابت‌افزار یا سفت‌افزار: برنامه‌ی نرم‌افزاری یا مجموعه‌ای از دستورالعمل‌های برنامه‌ریزی شده است که روی حافظه ROM یک دستگاه سخت‌افزاری قرار دارد. ثابت‌افزار دارای دستورالعمل‌های لازم برای نحوه‌ی ارتباط دستگاه با سایر سخت‌افزارهای رایانه‌ای است

هش کردن: فرآیند اعمال الگوریتم ریاضی روی مجموعه ای از داده‌ها برای تولید مقدار عددی (مقدار هش) برای نمایش داده هاست.

رابط‌های انسان و ماشین (HMI): به نرم‌افزار و سخت افزاری گویند که به اپراتورهای انسانی اجازه‌ی نظارت وضعیت یک فرآیند، تغییر تنظیمات و نحوه‌ی انجام عملیات خودکار به طور دستی در صورت بروز شرایط اضطراری را می‌دهند. این رابط‌ها همچنین به مهندس ناظر یا اپراتور اجازه می‌دهد تا نقاط تنظیم، الگوریتم‌ها و پارامترهای نظارتی را پیکربندی کند. کاربران مجاز از جمله مدیران، شرکای تجاری و اپراتورها می توانند با کمک این رابط‌ها به اطلاعاتی مانند وضعیت فرآیند، تاریخچه اطلاعات و گزارش‌ها دسترسی پیدا کنند.

طرح رویارویی با پیشامد: مجموعه‌ای از رویه‌های مستند و از پیش تعیین شده برای شناسایی و پاسخ به یک حادثه‌ی سایبری.

سازمان های به‌اشتراک‌گذارنده اطلاعات و تجزیه و تحلیل‌ها (ISAOs): هر نهاد رسمی، غیررسمی یا ائتلافی که توسط سازمان‌های بخش دولتی یا خصوصی ایجاد و به کار گرفته شود تا اهداف زیر را دنبال کند:

الف) جمع‌آوری و تجزیه و تحلیل اطلاعات زیرساخت‌های حیاتی برای درک بهتر مشکلات امنیتی و وابستگی‌های بین زیرساخت‌های حیاتی و سیستم‌های حفاظت شده؛ به طوری که از یکپارچگی، میزان در دسترس و قابل اعتماد بودن آن اطمینان حاصل شود.

ب) انتقال یا افشای اطلاعات زیرساخت حیاتی برای کمک به پیشگیری، شناسایی، کاهش یا بازیابی از اثرات ناشی از تداخل، سازش یا ناتوانی زیرساخت‌های حیاتی یا سیستم های حفاظت شده.

ج) توزیع داوطلبانه‌ی اطلاعات زیرساخت‌های حیاتی بین اعضا و دولت‌های ایالتی، محلی و فدرال یا هر نهاد دیگری که می تواند در به وقوع پیوستن اهداف ذکر شده کمک کند.

مراکز به‌اشتراک‌گذارنده‌ی اطلاعات و تجزیه و تحلیل‌ها (ISACs): یک نهاد عملیاتی قابل اعتماد که توسط مالکان و اپراتورهای زیرساخت های حیاتی بخش خصوصی با مشورت و کمک دولت فدرال (در صورت درخواست) ایجاد شده است تا به عنوان مکانیزمی برای جمع‌آوری، تجزیه و تحلیل، پاکسازی مناسب و انتشار اطلاعات مربوط به آسیب پذیری‌ها، تهدیدها، نفوذها و ناهنجاری‌ها به شرکای صنعتی و دولتی عمل کند. این مراکز به صورت بخش بخش عمل می کنند؛ به طوری که تاسیسات و سازمانهایی که در یک بخش از زیرساخت حیاتی خاص هستند، با هم همکاری می‌کنند و اطلاعات خود را درباره‌ی تهدیدات فیزیکی و سایبری و روش های مقابله به اشتراک می‌گذارند. اکثر مراکز، آگاهی موقعیتی بخش‌های خود را حفظ می‌کنند و هشدار درباره‌ی تهدیدات و گزارش رویدادها را به صورت شبانه‌روزی ارائه می‌دهند. برخی حتی سطوح تهدید برای بخش‌های خود تعیین می‌کنند. هدف مراکز این است که در تبادل مستقیم اطلاعات بین شرکت‌ها و دولت، تداخلی ایجاد نکنند.

فناوری اطلاعات (IT): به هر گونه تجهیزات یا سیستم به هم‌پیوسته یا زیرسیستمی گفته می‌شود که دستگاه اجرایی برای جمع‌آوری خودکار، ذخیره‌سازی، تجزیه و تحلیل، ارزیابی، دستکاری، مدیریت، حرکت، نظارت، نمایش، مبادله، انتقال یا دریافت داده و اطلاعات از آن استفاده می‌کند. این اطلاعات جمع آوری‌شده به طور مستقیم در دسترس دستگاه اجرایی یا افرادی که طبق قرارداد با دستگاه اجرایی مستلزم استفاده از آن تجهیزات هستند، قرار می‌گیرد.

کمیسیون بین‌المللی الکتروتکنیک (IEC): این یک سازمان عضویت جهانی و غیرانتفاعی است که ۱۷۳ کشور عضو آن هستند و بیست هزار کارشناس را گردهم آورده است. استانداردهای بین‌المللی IEC و برآورد میزان مطابقت فعالیت ها با قوانین، زیربنای تجارت بین‌المللی کالاهای الکتریکی و الکترونیکی را فراهم ساخته است. بنابراین، دسترسی به برق را تسهیل می‌کند و ایمنی، عملکرد و قابلیت همکاری دستگاه‌ها و سیستم‌های الکتریکی و الکترونیکی، از جمله دستگاه‌های مصرف‌کننده مانند تلفن‌های همراه یا یخچال‌ها، تجهیزات اداری و پزشکی، فناوری اطلاعات، تولید برق و موارد دیگر را تأیید می‌کند.

انجمن بین‌المللی اتوماسیون (ISA): این انجمن، یک انجمن حرفه‌ای غیرانتفاعی است که در سال ۱۹۴۵ برای ایجاد دنیایی بهتر از طریق اتوماسیون تاسیس شد. ISA با مرتبط ساختن جامعه‌ی اتوماسیون سعی در دستیابی به برتری عملیاتی است و قابل اعتمادترین ارائه‌دهنده‌ی منابع فنی پایه بر اساس استانداردهاست که به پیشرفت کسب و کارها و حرفه ای‌تر شدن آنها کمک می‌کند. این انجمن، توسعه‌دهنده‌ی استانداردهای جهانی پرکاربرد، ارائه‌دهنده‌ی گواهی به متخصصان، ارائه‌دهنده‌ی انواع آموزش مربوطه، منتشرکننده‌ی کتاب و مقالات فنی، فراهم‌کننده‌ی برنامه‌های شبکه‌سازی و توسعه‌ی شغلی برای اعضا و مشتریان خود در سراسر جهان است. همچنین ISA، میزبان کنفرانس‌ها و نمایشگاه‌هاست.

انجمن بین‌المللی اتوماسیون/کمیسیون بین‌المللی الکتروتکنیک (ISA/IEC) ۶۲۴۴۳: سری استانداردهای ISA/IEC ۶۲۴۴۳ توسط کمیته ISA۹۹ توسعه یافت و به تصویب کمیسیون بین‌المللی الکتروتکنیک (IEC) رسید. این سری استانداردها، چارچوبی منعطف برای رسیدگی و کاهش آسیب‌پذیری‌های امنیتی آینده در سیستم‌های اتوماسیون صنعتی و نظارتی ارائه می‌کند.

موجودی: فهرست رسمی یا سابقه اموال شخصی که به یک سازمان واگذار شده است.

فهرست آسیب‌پذیریهای قابل بهره‌برداری و شناخته شده (KEV): فهرستی از آسیب‌پذیری‌هایی که CISA شناسایی کرده است و مورد سوءاستفاده قرار گرفته‌اند. به عنوان بخشی از دستورالعمل‌های لازم‌الاجرا ۲۲-۰۱، شعب سازمان‌های اجرایی غیرنظامی فدرال (FCEB) موظفند که در چارچوب زمانی خاص این آسیب‌پذیری‌ها را اصلاح کنند تا امنیت زیرساخت‌ها تامین و میزان حملات سایبری کاهش یابد.

حداقل مزیت: این که یک چارچوب امنیتی طوری طراحی شود که هر نهادی از حداقل منابع سیستم و مجوزهای موردنیاز برای انجام فعالیت خود برخوردار باشد.

گزارش‌ها: ثبت حوادث رخ داده در سیستم‌ها و شبکه های یک سازمان.

ماکروهای آفیس مایکروسافت: ماکرو در اکسس، ابزاری است که امکان خودکارسازی وظایف و اضافه کردن قابلیت‌هایی را به فرم‌ها، گزارش‌ها و نحوه‌ی مدیریت فراهم می‌سازد. برای نمونه، اگر یک دکمه‌ی فرمان را به یک فرم اضافه کنید، رویداد آن‌کلیک (OnClick) دکمه به یک ماکرو مرتبط می‌شود و ماکرو حاوی دستوراتی است که با هر بار کلیک روی دکمه انجام می‌شود.

احراز هویت چندعاملی: احراز هویتی که بیش از یک فاکتور برای تأیید هویت ارائه می‌کند؛ مانند دستگاه احراز هویت رمزنگاری شده با حسگر بیومتریک که برای فعال کردن دستگاه موردنیاز است.

مؤسسه‌ی ملی استاندارد و فناوری (NIST): مؤسسه‌ی ملی استاندارد و فناوری با تشویق به نوآوری و افزایش رقابت صنعتی در ایالات متحده باعث پیشرفت علوم کمّی، استاندارد ها و فناوری در جهت افزایش امنیت اقتصادی و بهبود کیفیت زندگی می‌شود.

تقسیم‌بندی و جداسازی شبکه: تقسیم‌بندی شبکه شامل قطعه‌بندی یک شبکه به شبکه‌های کوچک‌تر است؛ در حالی که جداسازی شبکه، توسعه و اجرای مجموعه قوانینی برای کنترل ارتباطات بین میزبان‌ها و سرویس‌های خاص را شامل می‌شود.

چارچوب امنیت سایبری (CSF) NIST: مجموعه‌ای از فعالیت‌ها و مراجع امنیت سایبری که در بخش‌های زیرساخت حیاتی مشترک هستند و حول نتایج خاص سازماندهی می شوند. هسته‌ی چارچوب شامل چهار عنصر است: توابع، دسته بندی‌ها، زیرمجموعه‌ها و مراجع اطلاعاتی.

چارچوب مدیریت خطرات NIST: چارچوب مدیریت خطرات (RMF) که در NIST SP ۸۰۰-۳۷ آمده است، باعث ایجاد نظم و سازماندهی در یک فرآیند می‌شود تا فعالیت‌های مربوط به امنیت اطلاعات و مدیریت خطرات در یک سیستم در یک راستا قرار بگیرد.

NIST SP ۸۰۰-۳۰: راهنمایی برای انجام ارزیابی خطرات و تهدیدات سیستم‌ها و سازمان‌های فدرالی ارائه می‌دهد. ارزیابی خطراتی که در هر سه سطح از سلسله‌مراتب مدیریت خطرات انجام می‌شود، بخشی از یک فرآیند کلی است که اطلاعات لازم را برای مدیران ارشد در مقابله با خطرات شناسایی شده ارائه می‌دهد.

NIST SP ۸۰۰-۵۳: شامل مواردی برای کنترل سیستم‌ها و سازمان‌هاست. از آن می‌توان در هر سازمان یا سیستمی که اطلاعات را پردازش، ذخیره یا انتقال می‌دهد، بهره برد. استفاده از این موارد کنترلی برای سیستم‌های اطلاعاتی فدرال اجباری است و در واقع مجموعه‌ای از موارد کنترل‌های امنیتی و حریم خصوصی برای برآوردن نیازهای حفاظتی فعلی و آتی بر اساس تهدیدات، آسیب‌پذیری‌ها، الزامات و فناوری‌های در حال تغییر و پیشرفت است. بنابراین، ارتباط بین سازمان‌ها به دلیل وجود موارد مشترک در زمینه‌های امنیتی، حریم خصوصی و مدیریت خطرات، قوی‌تر می‌شود.

NISTSP ۸۰۰-۸۲: راهنمایی برای ایمن‌سازی سیستم‌های کنترل صنعتی (ICS)، از جمله سیستم‌های کنترل نظارتی و جمع‌آوری داده‌ها (SCADA)، سیستم‌های کنترل توزیع شده (DCS) و دیگر سیستم‌هایی که عملکردهای کنترلی را انجام می‌دهند، ارائه می‌کند. همچنین سندی است که علاوه بر نمایانگر بودن کلیت ICS، توپولوژی‌ها و معماری معمولی سیستم را بررسی می‌کند، تهدیدات و آسیب‌پذیری‌های شناخته شده را شناسایی می‌کند و اقدامات متقابل امنیتی برای کاهش خطرات ذکر شده ارائه می‌دهد.

فناوری عملیاتی (OT): به سیستم‌ها یا دستگاه‌هایی گفته می‌شود که می‌توان آنها را برنامه‌ریزی کرد تا با محیط فیزیکی در تعامل باشند (یا دستگاه‌هایی را که با محیط فیزیکی در تعامل هستند، مدیریت کنند). این سیستم‌ها یا دستگاه‌ها با نظارت یا کنترل دستگاه‌های دیگر، فرآیندها و حوادث، تغییر و تحولات را شناسایی یا مستقیما باعث ایجاد تغییرات می‌شوند. از جمله این سیستم‌ها می‌توان به سیستم کنترل صنعتی، سیستم مدیریت ساختمان، سیستم کنترل حریق و مکانیزم‌های کنترل دسترسی فیزیکی اشاره کرد.

تست نفوذپذیری (از راه دور): شبیه‌سازی‌ای از نحوه و روش‌های سوءاستفاده از راه‌های نفوذپذیر است. این شبیه سازی برای آزمایش خطوط دفاعی، تست امنیت برنامه‌های کاربردی و تخمین احتمال سوءاستفاده از اطلاعات منبع باز، کمک می‌کند.

فیشینگ: شکل دیجیتالی مهندسی اجتماعی است که افراد را فریب می‌دهد تا خودشان اطلاعات حساس را ارائه کنند.

حساب ممتاز: یک حساب سیستم اطلاعاتی با مجوز تأیید شده است که اغلب حساب ادمین هم نامیده می‌شود.

پروتکل دسترسی از راه دور به دسکتاپ (RDP): پروتکل اختصاصی مایکروسافت است که اتصال از راه دور به رایانه‌های دیگر از طریق پورت TCP ۳۳۸۹را فعال می‌کند و کاربر می‌تواند به کمک یک کانال رمزگذاری شده، از راه دور به شبکه دسترسی پیدا کند. مدیران شبکه از RDP برای شناسایی مشکلات، ورود به سرورها و دیگر فعالیت‌های از راه دور استفاده می‌کنند. کاربران هم از این پروتکل برای ورود به شبکه سازمان جهت دسترسی به ایمیل و فایل‌ها از راه دور بهره می برند.

سالتینگ گذرواژه: اضافه شدن یک رقم تصادفی به گذرواژه برای پیچیده‌تر کردن آن. معمولا گذرواژه‌ها به الگوریتم هشینگ سپرده شده و نتایج در دیتابیسِ ورود به سیستم ذخیره می‌شود. زمانی که کاربران گذرواژه خود را وارد می‌کنند، آن گذرواژه بار دیگر هش شده و با آنچه در دیتابیس ذخیره شده است، مقایسه می‌شود. «سالت» در واقع یک رقم تصادفی است که قبل از هش شدن به گذرواژه اضافه می‌شود تا کشف شدن آن دشوار گردد.

معماری سیستم: معماری عبارت است از اساس سازمانی یک سیستم که در اجزای آن، روابط اجزا با یکدیگر و با محیط، اصول حاکم بر طراحی و تکامل وجود دارد.

Table-Top Exercise (TTX): جمعی از پرسنل با مسئولیت‌های متفاوت در حوزه‌ی فناوری اطلاعات گردهم می آیند تا در رابطه با طرح‌های ارائه شده و مسئولیت‌هایشان در صورت بروز شرایط اضطراری و نحوه‌ی پاسخگویی بحث کنند. یک نفر که مدیریت‌کننده و شروع‌کننده‌ی بحث است، سناریویی را ارائه و سؤالاتی بر اساس آن طرح می‌کند.

امنیت لایه‌ی انتقال (TLS): یک پروتکل احراز هویت و رمزگذاری است که به طور گسترده در مرورگرها و سرورهای وب اجرا می‌شود. ترافیک HTTP که با TLS منتقل شده است، به عنوان HTTPS شناخته می‌شود.

برنامه‌ی افشای آسیب‌پذیری: حاوی دستورالعمل‌های واضح برای محققان امنیتی جهت کشف آسیب‌پذیری‌ها و نحوه‌ی استفاده از یافته‌ها در سطح سازمانی است.