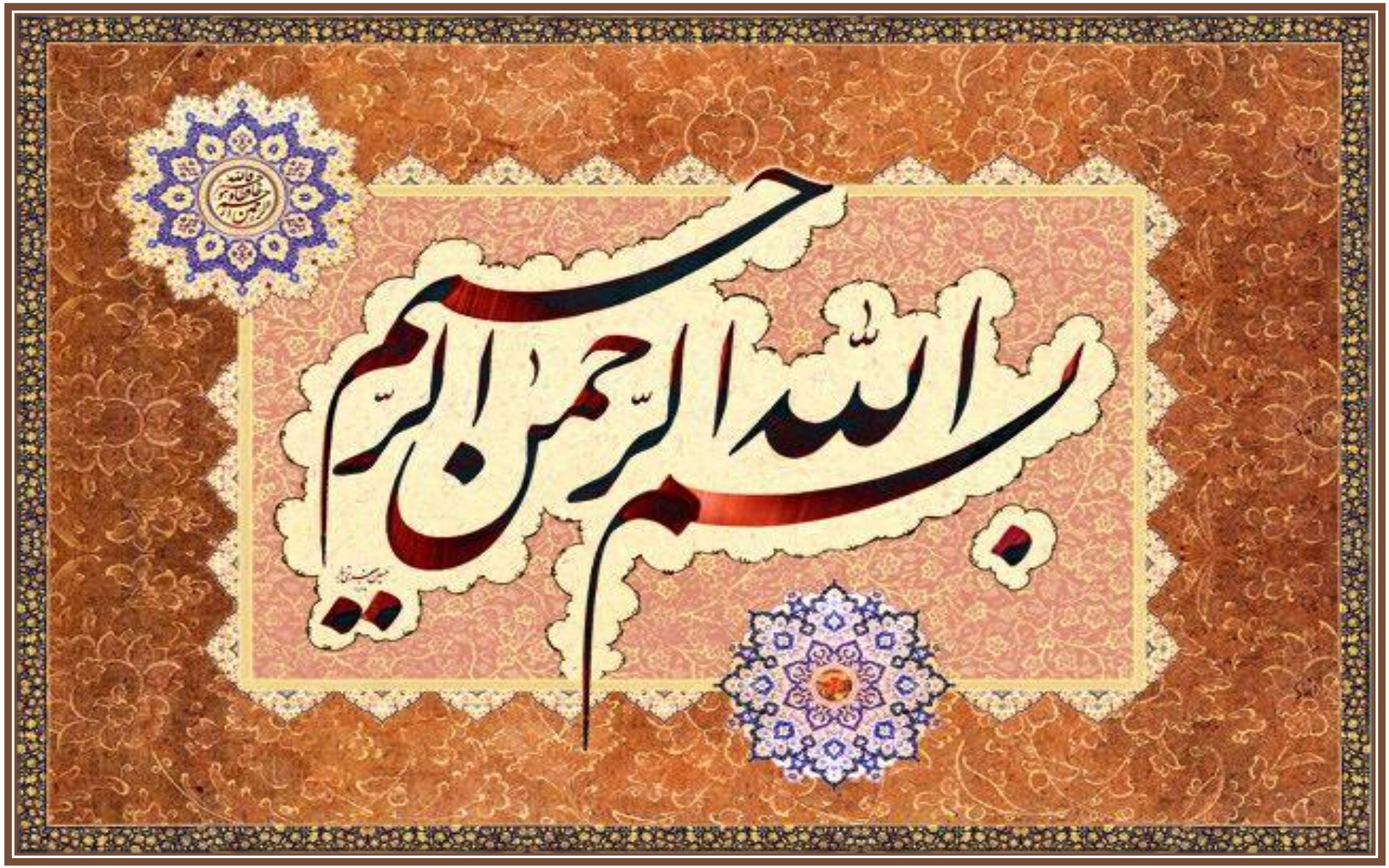

بسم الله الرحمن الرحیم

سازمان پدافند غیرعامل کشور

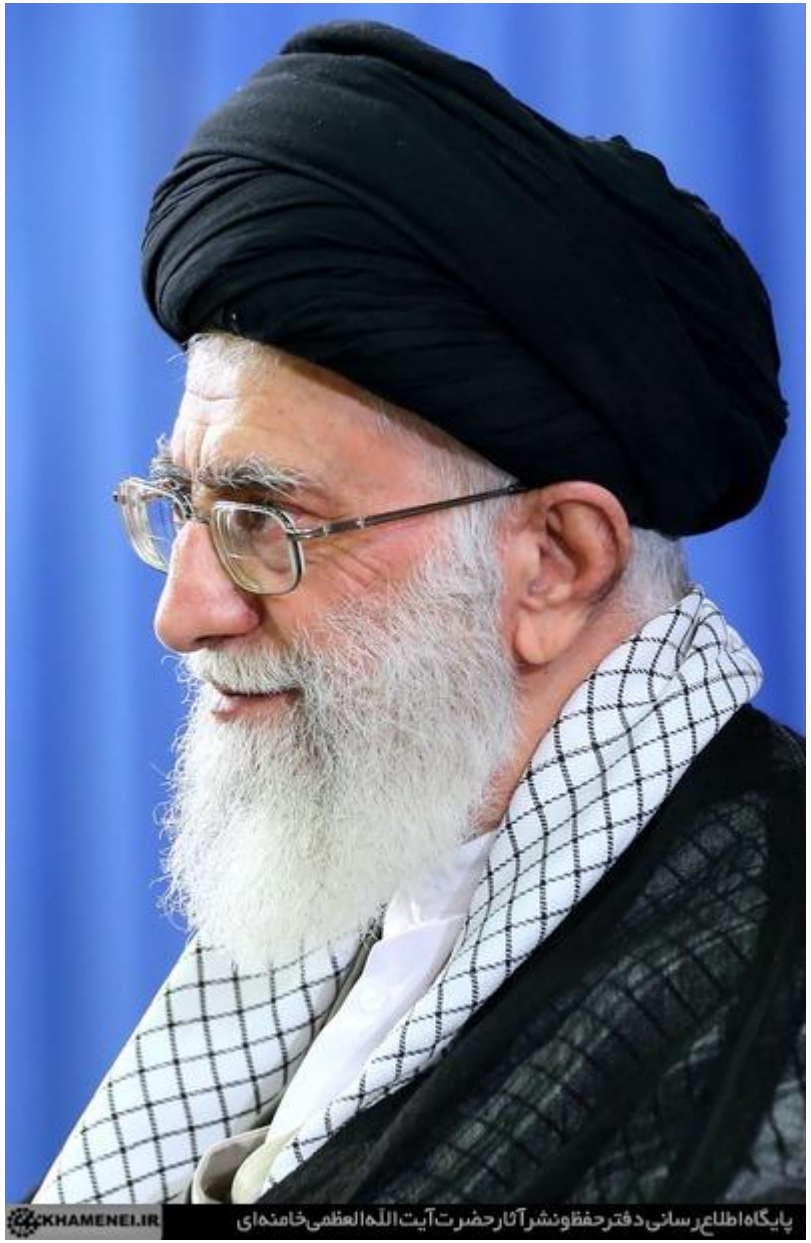
امنیت سایبری

دکتر محمدرضا موحدی صفت

عضو هیات علمی دانشگاه عالی دفاع ملی

مرداد ۱۴۰۱

فضای مجازی واقعاً یک دنیای رو به رشدِ غیرقابل توقّف است ... این یک فرصت‌های بزرگی در اختیار هر کشوری میگذارد، تهدیدهایی هم در کنارش دارد؛ ما بایستی کاری کنیم که از آن فرصتها حدّاکثر استفاده را بکنیم، از این تهدیدها تا آنجایی که ممکن است خودمان را برکنار نگه بداریم.



بیانات فرماندهی معظم کل قوا در دیدار اعضای هیات دولت ۱۳۹۵

لایه های اصلی فضای سایبر

لایه زیرساخت

- زیرساخت های ارتباطی
- زیرساخت های اطلاعاتی
- تجهیزات و سخت افزارها
- شبکه ها
- مخابرات و ارتباطات
- مراکز داده
- .....

لایه سرویس و خدمات

- برنامه های کاربردی
- خدمات پایه و ابزارهای ضروری
- سکوها و پلتفرم ها
- خدمات عمومی و الکترونیکی
- ...

لایه محتوا و داده

- پشتیبانی از انواع داده ها
- داده کاوی
- مدیریت اطلاعات و دانش
- یکپارچگی داده ها
- ...

لایه کاربران

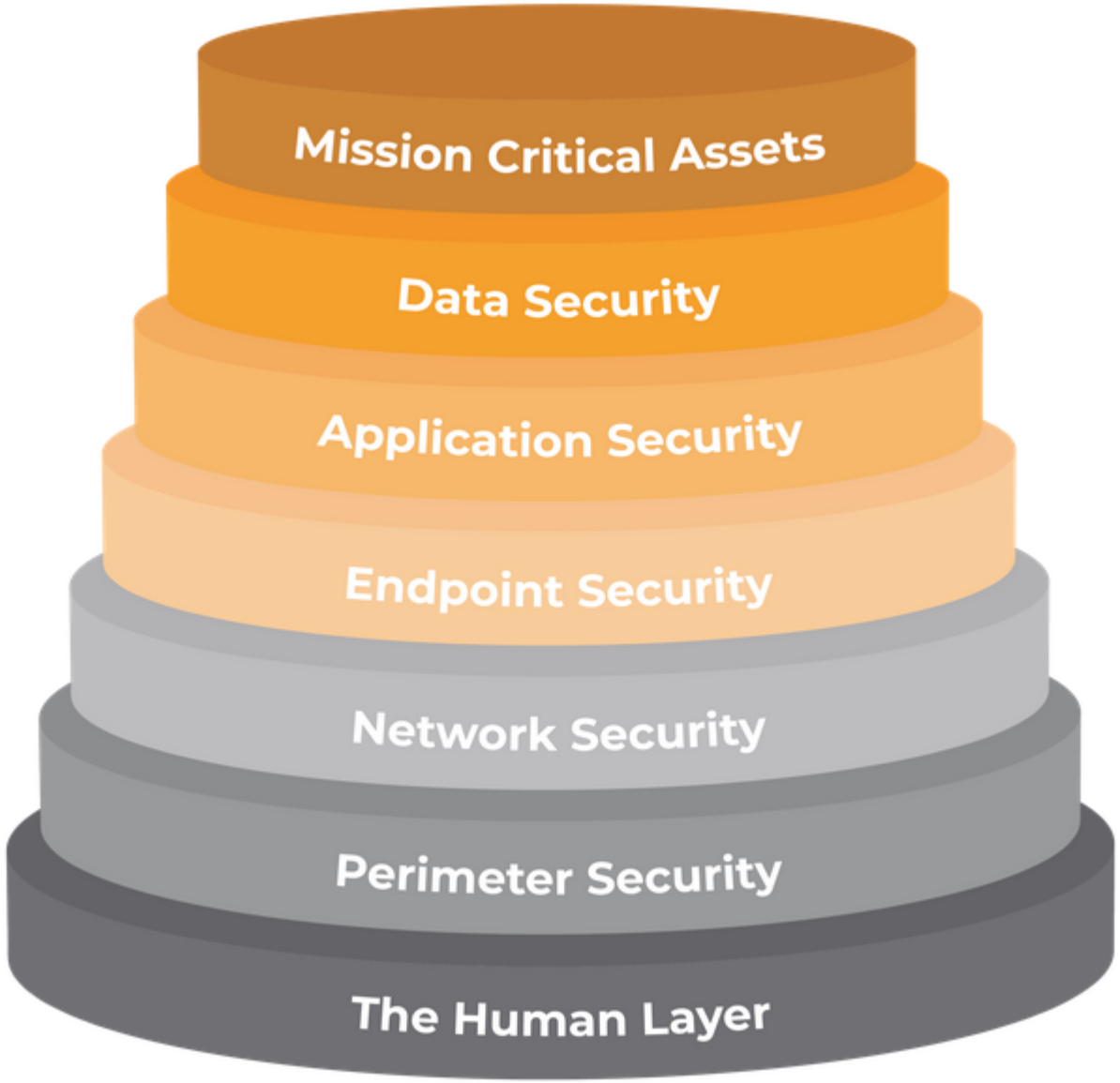
- کارکنان سازمان
- اعضاء
- ذینفعان
- سازمان های متعامل
- .....

لایه مدیریت

- مدیریت فضای سایبر سازمان
- حاکمیت فضای سایبر
- حکمرانی در فضای سایبر
- حاکمیت داده ها
- .....

لایه شناختی

- علوم شناختی، علمی است میان رشته‌ای از روانشناسی، علوم محاسباتی، زبان‌شناسی، فلسفه و علوم اعصاب برای درک کارکرد ذهن انسان.
- بسیاری از حملات سایبری با بهره‌گیری از محدودیت‌های شناختی عامل انسانی و از طریق عمل بر روی ذهن و اندیشه کاربران شکل می گیرد.



لایه امنیت

- امنیت در لایه زیرساخت
- امنیت در حوزه سرویس و خدمات
- امنیت در داده و محتوا
- امنیت کاربران
- .....

امنیت در فضای سایبر

- امنیت در حوزه های اقتصادی
  - کسب و کارهای سایبری
  - رمز ارزها
  - ....
- امنیت در حوزه های اجتماعی
  - شبکه های اجتماعی
  - پیام رسان ها
  - .....

امنیت در فضای سایبر

- دفاعی – امنیتی (جنگ سایبری)
  - سایبر در رزم
  - رزم سایبری
  - ....
- امنیت فرهنگی (حوزه های نرم و شناختی)
  - جنگ نرم
  - جنگ رسانه ای
  - ....

امنیت در فضای سایبر

- امنیت سیاسی
  - مرز سایبری
  - تعاملات بین الملل در حوزه سایبر
  - ....
- امنیت حوزه فناوری
  - امنیت زیرساخت ها
  - امنیت شبکه ها
  - .....

امنیت در فضای سایبر

- امنیت حقوقی
  - دیپلماسی بین المللی
  - حقوق و قوانین در فضای سایبر
  - ....
- امنیت زیست محیطی
  - ❑ فناوری های زیستی
  - ❑ بیوتروریسم سایبری
  - .....

تعاریف اولیه:

امنیت رایانه ای (Computer Security):

حفاظت از سیستم های اطلاعاتی خودکار به منظور دستیابی به اهداف قابل استفاده برای حفظ یکپارچگی، دسترسی و محرمانه بودن منابع سیستم اطلاعاتی (شامل سخت افزار، نرم افزار، میان افزار، اطلاعات/ داده ها، ارتباطات و ....) می باشد.

حمله (Attack):

به تلاش عمدی برای رخنه در یک سیستم یا سوء استفاده از آن اطلاق می گردد.

رخنه (Breach):

به نقض سیاست امنیتی در یک سیستم گفته می شود.

نفوذ (Intrusion):

به فرآیند حمله و رخنه ناشی از آن اطلاق می گردد.

تعاریف اولیه:

آسیب پذیری (Vulnerability):

نقطه ای از سیستم است که احتمال رخنه از آنجا وجود دارد.

هک (Hack):

کنکاش به منظور کشف حقایق و نحوهٔ کار یک سیستم است. درواقع حمله (Attack) تلاش برای نفوذ به سیستمهای دیگران و نوعی هک خصمانه است.

حمله امنیتی (Security Attack):

عملی که امنیت اطلاعات سازمان را نقض می کند.

مکانیزم امنیتی (Security Mechanism):

روش در نظر گرفته شده برای تشخیص، جلوگیری و بازیابی از حملات می باشد.

سرویس امنیتی (Security Service):

به سرویس های تضمین کننده امنیت با استفاده از مکانیزم های بالا گفته می شود.

تعاریف اولیه:

آگاهی رسانی، پشتیبانی و امداد (آپا):

عنوان « امداد و نجات کامپیوتری » یا «مدیریت رخدادهای ام نیتی»، مورد استفاده قرار گرفته معادل اختصار(CERT)و دیگر اختصارات مترداف آن مورد استفاده قرار گرفته و عبارت است از: یک قابلیت سازمانی که مسئولیت پیشگیری، بررسی و پاسخگویی به حوادث امنیت کامپیوتری را در جامعه قلمرو به عهده دارد.

مدیریت حادثه:

مدیریت حادثه عبارت است از قابلیت شناسایی، ردیابی، تجزیه و تحلیل و پاسخگویی سریع و بهنگام به حوادث کامپیوتری در یک سازمان ک با ایجاد زیرساختهای لازم، آمادگیهای سازمانی جهت مواجهه با تهدیدات کامپیوتری سازمان یافته، هکرهای حرفه ای و نفوذگرهای داخلی را میسر می نماید.

تعاریف اولیه:

مرکز عملیات امنیت

یک واحد متمرکز در سازمان که با مشکلات امنیتی سرو کار داشته و دارای نیروی انسانی و تجهیزات مورد نیاز برای نظارت و پایش امنیت سیستم های فناوری اطلاعات و ارتباطات سازمان است.

مدیریت حادثه:

مدیریت حادثه عبارت است از قابلیت شناسایی، ردیابی، تجزیه و تحلیل و پاسخگویی سریع و بهنگام به حوادث کامپیوتری در یک سازمان ک با ایجاد زیرساختهای لازم، آمادگیهای سازمانی جهت مواجهه با تهدیدات کامپیوتری سازمان یافته، هکرهای حرفه ای و نفوذگرهای داخلی را میسر می نماید.

سیستم مدیریت امنیت اطلاعات:

استانداردهای مدیریت امنیت فضای تبادل اطلاعات، تعدادی استاندارد امنیتی است که به سازمان‌ها توان اجرای تکنیک‌ها و سیاست‌هایی را می‌دهد تا تعداد حملات موفق در فضای تبادل اطلاعات به حداقل برسد. در واقع این استانداردها یک چارچوب امنیتی کلی و یک سری تکنیک‌های تخصصی برای پیاده سازی «امنیت» در فضای تبادل اطلاعات فراهم می‌کنند.

سرویس های امنیتی:

احراز هویت (Authentication)

- تضمین اینکه موجودیت ارتباطی همان است که ادعا می کند. (احراز هویت موجودیت ها – احراز هویت مبداء داده)
- احراز هویت فرآیندی است که طی آن درستی هویت یک فرد شناسایی و تأیید می‌گردد. بنابراین زمانی که کاربر بخواهد وارد سیستم شده و یا به منبعی دسترسی پیدا کند، ابتدا باید خود را اثبات کند.

سرویس های امنیتی:

روش های احراز هویت

- **روش اول**

استفاده از کلمات عبور

روش دوم

احراز هویت دوعاملی (هویت پیامکی)

- **روش سوم**

احراز هویت مبتنی بر توکن

- **روش چهارم**

احراز هویت براساس ویژگی‌های منحصربه‌فرد هر فرد انجام می‌شود.اثر انگشت، تشخیص چهره، قرنیه، الگوی صحبت کردن شما، حرکت چشم‌ها و ....

سرویس های امنیتی:

یکپارچگی (Integrity)

- یکپارچگی داده به معنی صحت، کامل بودن و سازگاری کلی داده‌ها است.
- یکپارچگی داده ها این است که اطمینان حاصل کنیم که داده ها "نامتناقض" و "صحیح" هستند.

سرویس های امنیتی:

یکپارچگی (Integrity)

- یکپارچگی در زیرساخت
- یکپارچگی در تجهیزات
- یکپارچگی سامانه ها
- یکپارچگی داده ها و اطلاعات
- یکپارچگی در سرویس های امنیتی

سرویس های امنیتی:

کنترل دسترسی (Access Control)

Object / Subject	File 1	File 2	File 3	File 4
User 1	Read	Write	Own	-
User 2	Write	Own	-	-
User 3	Own	-	-	Read
User 4	Read	Read	Read	Own

- جلوگیری از استفاده غیر مجاز از یک منبع. کنترل می کند ۱– چه کسی به منبع دسترسی دارد؟ ۲– تحت چه شرایطی دسترسی اتفاق می افتد؟ ۳– کدام دستیابی ها به منبع مجاز است؟
- تضمین‌کننده این مطلب است که کاربران مجاز سیستم می‌توانند دسترسی به موقع و بی‌وقفه به اطلاعات سیستم داشته باشند.

سرویس های امنیتی:

کنترل دسترسی (Access Control)

- از طریق اهداف زیر بیان می‌گردد:
  - ✓ ممانعت از تغییر اطلاعات توسط افراد غیرمجاز.
  - ✓ ممانعت از تغییر غیرعمدی توسط افراد مجاز
  - ✓ محافظت از سازگاری داخلی و خارجی

کنترلها می‌توانند به سه صورت: ممانعت، تشخیص و تصحیح باشند.

کنترلهای ممانعتی جهت جلوگیری از وقایع مضر بکار گرفته می‌شوند، کنترلهای تشخیصی برای کشف وقایع مضر ایجاد شده‌اند و کنترلهای تصحیحی برای بازیابی سیستم‌هائی که مورد حمله‌های مضر واقع شده‌اند، استفاده می‌شوند.

سرویس های امنیتی:

- **محرمانگی (Confidentiality)**
- محافظت در برابر افشاء غیرمجاز است. شامل محافظت در همه لایه های فضای سایبر از همه داده های کاربر در یک اتصال – محرمانگی فیلدها در داخل داده های کاربر – محافظت از اطلاعاتی که در مشاهده جریان های ترافیکی به دست می آید

سرویس های امنیتی:

محرمانگی (Confidentiality)

- محرمانگی زیرساخت ها در سازمان ها
- محرمانگی تجهیزات
- محرمانگی برای سامانه ها
- محرمانگی داده ها و اطلاعات

سرویس های امنیتی:

- **عدم انکار** (non repudiation)

- **محافظت در برابر افشاء غیرمجاز است. شامل محافظت در همه لایه های فضای سایبر از همه داده های کاربر در یک اتصال – محرمانگی فیلدها در داخل داده های کاربر – محافظت از اطلاعاتی که در مشاهده جریان های ترافیکی به دست می آید**

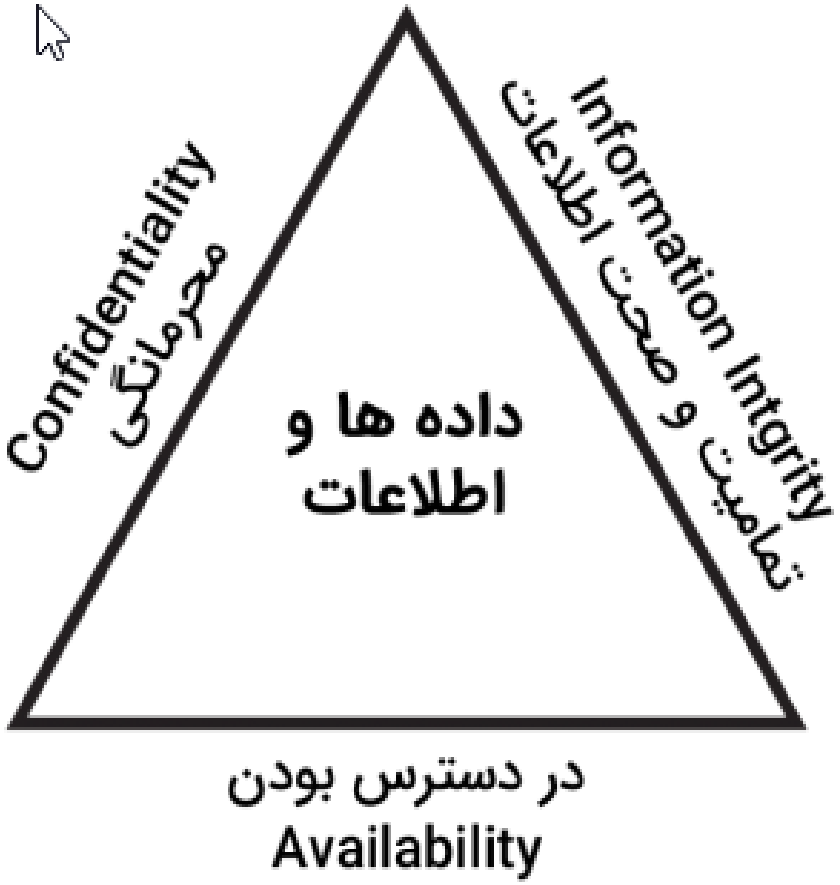
سرویس های امنیتی:

- **عدم انکار** (non repudiation)

یک روش برای شناسایی و تأییدِ هویت‌ها به صورت قطعی و قابل قبول و غیرقابل جعل

- هم از جعل سند و هویت و هم از انکار احتمالی آن در آینده جلوگیری می‌شود
- شناسایی و تأییدِ هویت و اصالتِ منبع اطلاعات نیز با استفاده از زیرساخت کلید عمومی، امضای رقومی، احراز هویت چندعاملی و اختصاص گواهی رقومی به افراد و سازمان‌ها انجام می‌گردد.

سرویس های امنیتی:



- **دسترس پذیری (Availability)**

- **هرگاه کاربر درخواست نماید، سرویس ها در اختیار وی قرار گیرد.**

سرویس های امنیتی:

- **دسترس پذیری (Availability)**
- **باز بودن درگاه های دسترسی بعد از حصول از امنیت**
- **باید احراز هویت و کنترل دسترسی به عنوان دو فاکتور مهم توسط مدیر امنیت سایت لحاظ شود**

یک قرارداد سطح خدمات (SLA) انتظارات بین ارائه‌دهنده خدمات و مشتری را تعیین می‌کند و محصولات یا خدماتی را که قرار است ارائه شوند و همچنین نقطه تماس واحد برای مشکلات کاربر نهایی و معیارهایی که اثربخشی فرآیند را بر اساس آن تعیین می‌کند را توصیف می‌کند.

سرویس های امنیتی:

- **حریم خصوصی (Privacy)**

- یعنی یک فرد یا گروه بتواند خود یا اطلاعات مربوط به خود را مجزا کند و در نتیجه بتواند خود یا اطلاعاتش را با انتخاب خویش در برابر دیگران آشکار کند
- حریم شخصی باعث می‌شود که هر فرد بتواند هویت، عقاید، نگرش و احساسات خاص خود را داشته باشد.

سرویس های امنیتی:

- **حریم خصوصی (Privacy)**

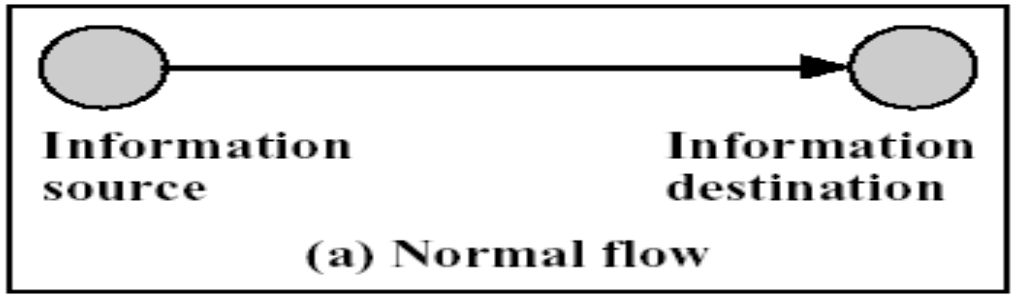
- حریم شخصی گاه مربوط به ناشناس بودن، یعنی تمایل به گمنام یا دور ماندن از عرصه عمومی است
- انواع مختلفی از حریم نظیر حریم شخصی مالی، حریم شخصی سلامتی، حریم شخصی برخط و حریم شخصی اطلاعاتی تعریف شده‌است
- قانون حریم داده های الکترونیکی در مجلس تصویب شده است

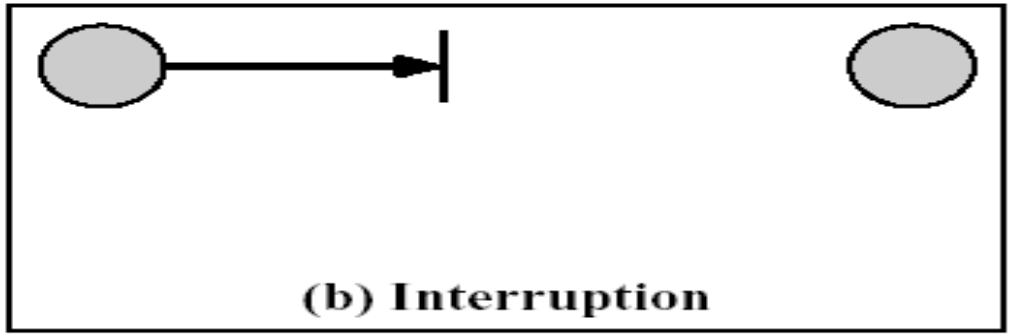
سرویس های امنیتی:

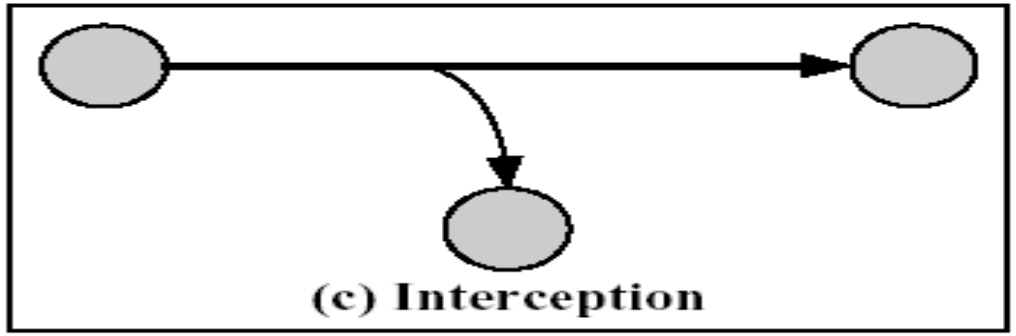
اعتماد (Trust)

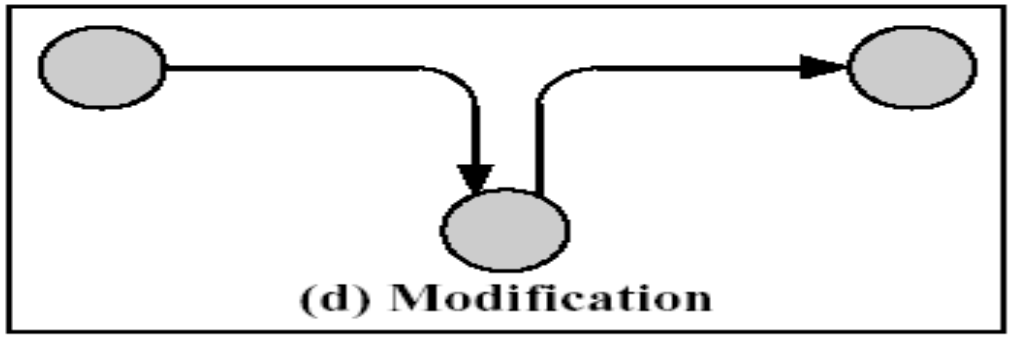
- اطمینان از درستی عملکرد سیستم
- یک رابطه حقوقی است که در آن دارنده حق آن
- را به شخص یا نهاد دیگری می دهد که باید آن را حفظ کند و صرفاً به نفع دیگری استفاده کند.

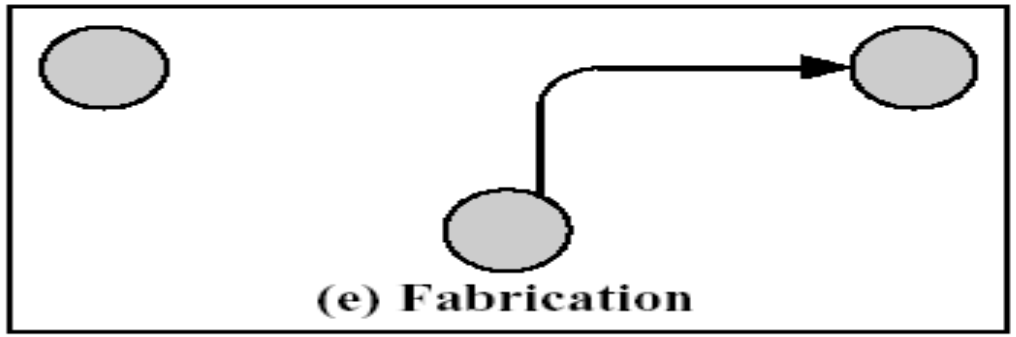
سناریوهای حمله











چالش های استقرار امنیت در سیستم ها:

- ✓ امنیت بالا، هزینه بر است.
- ✓ معمولا باعث کاهش کارایی سیستم ها می شود.
- ✓ نیاز به نظارت منظم دارد.
- ✓ کاربران آن را به عنوان مانع تلقی کرده و از سیاست های امنیتی تبعیت نمی کنند.

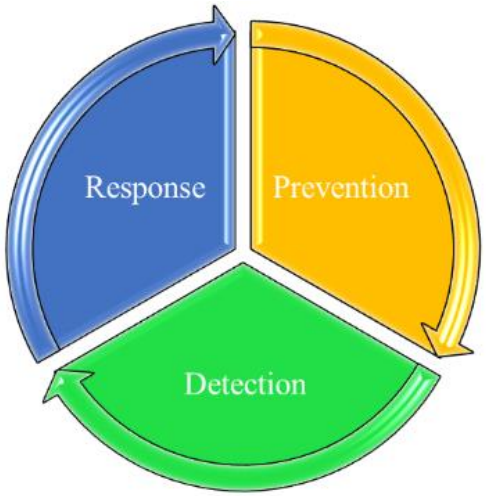
چالش های استقرار امنیت در سیستم ها:

- ✓ نرم افزارهای دور زدن امنیت به طور گسترده در دسترس است.
- ✓ ملاحظات و پیوست های امنیتی در مراحل مختلف تولید سیستم ها بکارگرفته نمی شود.
- ✓ برخی دورزدن امنیت را به عنوان یک مبارزه در نظر گرفته و از آن لذت می‌برند. (پروژه های دانشجویی)
- ✓ تجهیزات بومی در حوزه های زیرساخت فضای سایبر ملی وجود ندارد.

چالش های استقرار امنیت در سیستم ها:

- ✓ مدیران سازمان ها به اهمیت امنیت سامانه ها توجه کافی را ندارند.
- ✓ آموزش به کاربران در سطوح مختلف در سازمان ها اعمال نمی شود.
- ✓ بروز رسانی ها در بخش های زیرساخت و سامانه های خدماتی با فواصل طولانی انجام می شود.
- ✓ آزمایشگاه های کافی و قوی برای تست امنیت در حوزه های مختلف وجود ندارد.

اقدامات امنیتی



- ممانعت:
  - جلوگیری از خسارت
- ردیابی:
  - تشخیص
    - میزان خسارت
    - هویت دشمن
    - کیفیت حمله (زمان، مکان، دلایل حمله، نقاط ضعف...
- واکنش:
  - بازیابی و جبران خسارات
  - جلو گیری از حملات مجدد

خدمات امنیتی

- خدمت امنیتی:
  - یک خدمت پردازشی یا ارتباطی از سیستم؛
  - جهت فراهم آوردن نوع مشخصی از محافظت برای منابع سیستم.
- **مثال:**
  - خدمت کنترل دسترسی
  - خدمت محرمانگی داده
  - خدمت تصدیق هویت موجودیت

سازوکار امنیتی

- یک روش، فرآیند یا ابزار؛
- جهت پیاده‌سازی یک خدمت امنیتی؛
- که توسط یک سیستم یا درون آن فراهم می‌شود.
- **مثال:**
  - رمزنگاری
  - امضای رقمی
  - دیوار آتش

سیاست امنیتی

- یک هدف، مسیر یا روش اقدام مشخص؛
- برای تعیین و جهت‌دهی به تصمیمات حال و آینده؛
- در رابطه با امنیت در یک سیستم.

- **مثال:**
  - سیاست امنیتی نصب نرم‌افزار
  - سیاست امنیتی ساخت گذرواژه
  - سیاست امنیتی دسترسی راه دور

تعریف تهدید سایبری

- یک عامل خارجی
  - با قابلیت وارد نمودن ضربه به ماموریت‌ها و وظایف یک سازمان، کارکنان سازمان یا سرمایه سایبری
- از طریق دسترسی غیرمجاز
- انهدام (تخریب)
- افشاء
- تغییر اطلاعات
- ممانعت یا ایجاد اختلال در ارائه خدمت

تعریف تهدید سایبری

- عامل خارجی با قابلیت وارد نمودن ضربه به امنیت ملی، اقتصاد ملی، وجهه کشور در سطح بین المللی، روابط سیاسی و اقتصادی کشور، سلامت و ایمنی عمومی، اطمینان عمومی، باورهای دینی ملی یا اداره امور کشور، از طریق تخریب یا ایجاد اختلال گسترده در عملکرد زیرساخت‌های حیاتی، حساس یا مهم کشور.

آسیب پذیری ها و مخاطرات فضای سایبر

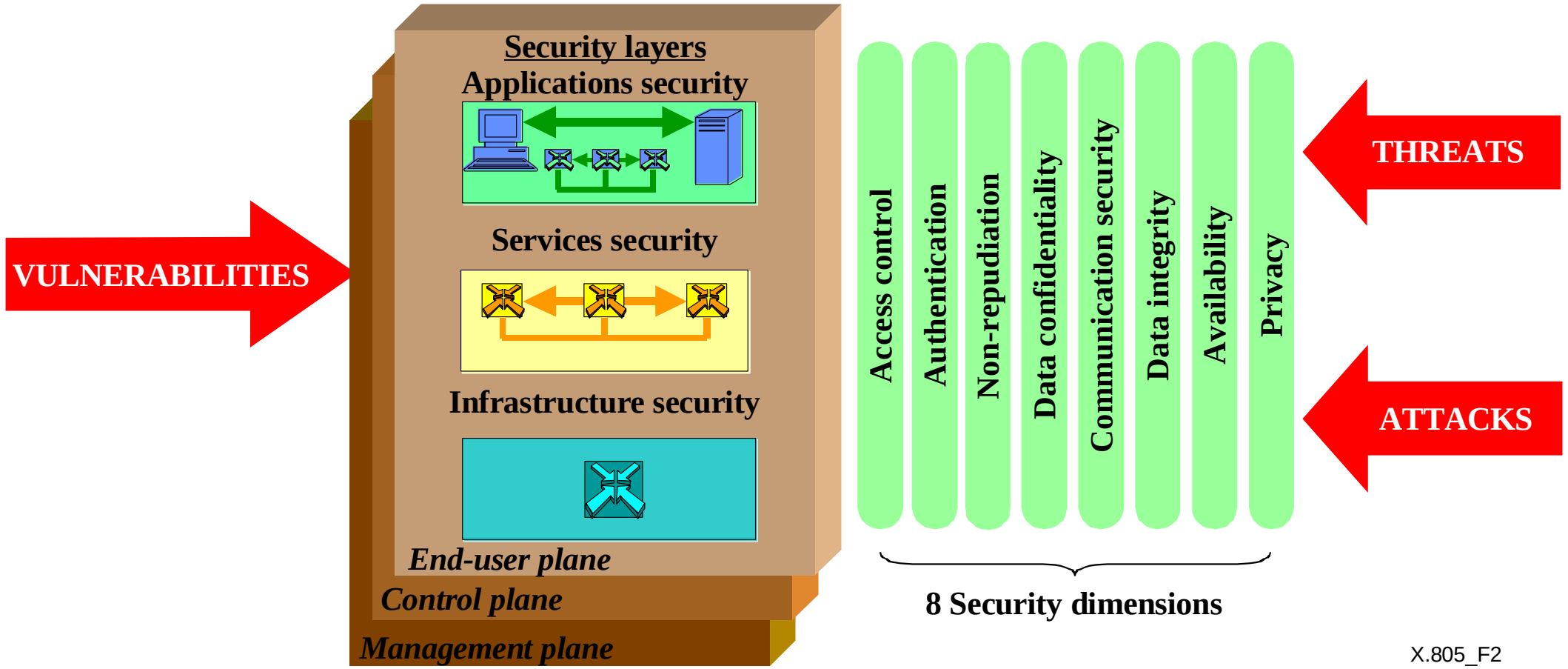
- آسیب‌پذیری، به ضعف موجود در داخل یک سرمایه، رویه های امنیتی یا کنترل های داخلی، یا پیاده سازی آن سرمایه که قابلیت بهره برداری یا فعال شدن توسط یک تهدید خارجی را داشته باشد اطلاق می‌گردد.

آسیب پذیری ها و مخاطرات فضای سایبر

- آسیب پذیری سایبری، آسیب پذیری موجود در اجزاء یک زیرساخت است که قابلیت بهره برداری یا فعال شدن توسط یک تهدید سایبری را داشته باشد.

- نقطه ای از سیستم است که احتمال رخنه از آنجا وجود دارد. همچنین عبارت است از "هرگونه ضعف در سیستم که قابل سوء استفاده باشد".

آسیب پذیری ها به لایه ها و مولفه های امنیتی:



مهمترین منشاء آسیب پذیری های سایبری موارد ذیل می باشند:

- فناوری (Technology)
- پروسه ها (Process)
- کاربران (Users)
- طراحی (Design)

تهدیدات لایه یکم : تهدیدات فیزیکی و امنیت فیزیکی

تهدیدات لایه دوم : تهدیدات لایه سوئیچ ها، Access Pointها و کلیه دستگاه های لایه دو

تهدیدات لایه سوم : تهدیدات مربوط به آدرس دهی IPو مسیریابی و فایروال ها

تهدیدات لایه چهارم : تهدیدات مربوط به دستگاهی بسته های اطلاعات و شنود شبکه

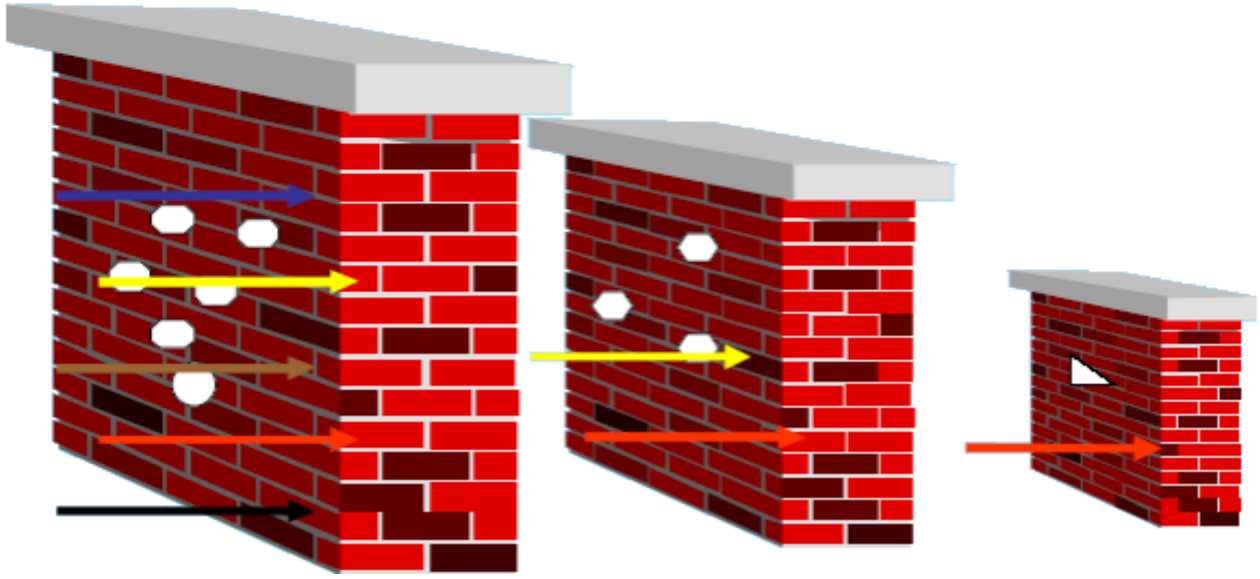
تهدیدات لایه پنجم : تهدیدات مربوط به استراق سمع و ورود به Session اطلاعاتی

تهدیدات لایه ششم : تهدیدات مربوط به الگوریتم های رمزنگاری و رمزنگاری نادرست اطلاعات

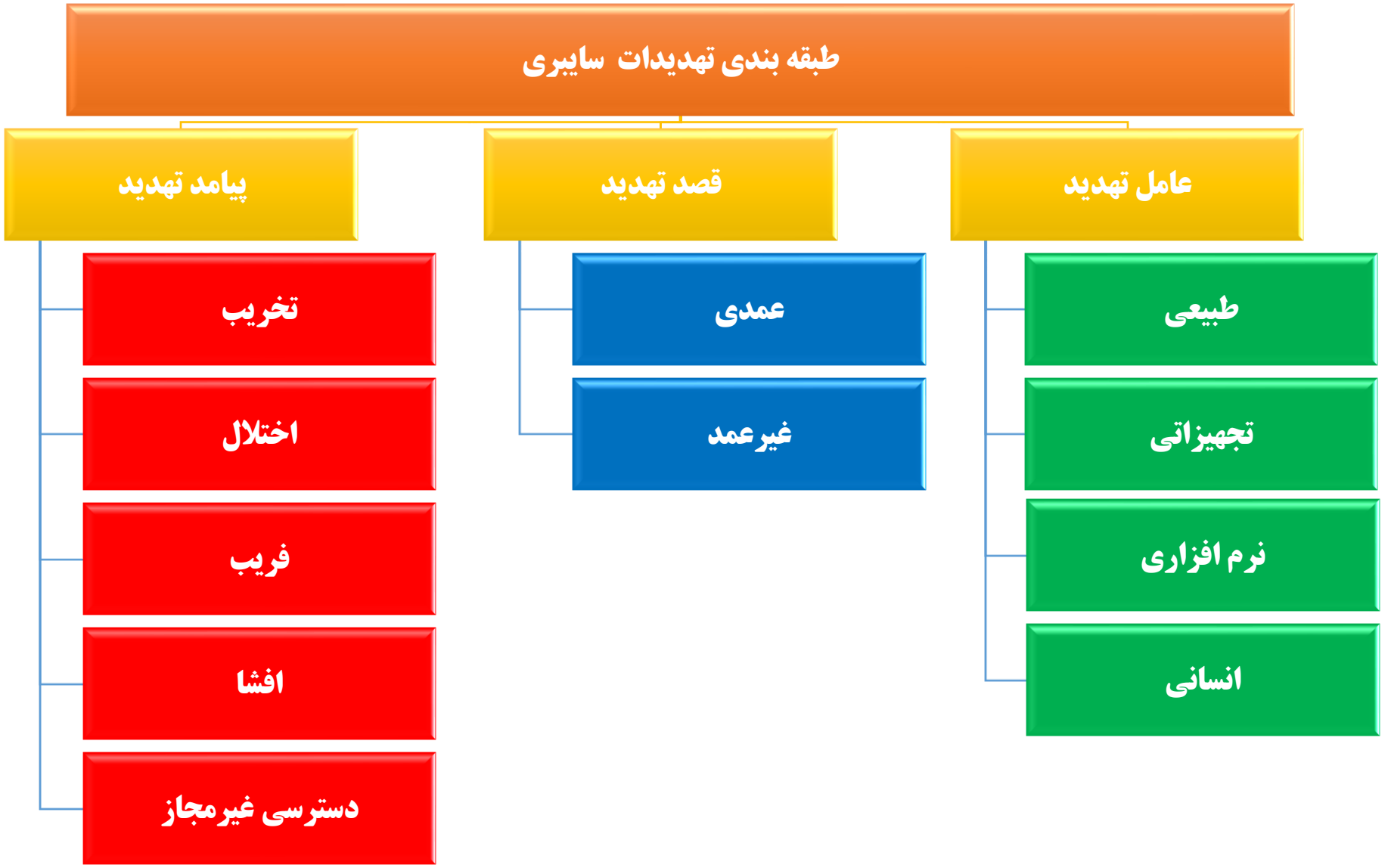
تهدیدات لایه هفتم : تهدیدات مربوط به نرم افزارهای کاربردی

روش های تامین امنیت:

- **دفاع چند لایه (دفاع چند لایه):** افزایش تعداد لایه‌های دفـاعی و دشوار کردن مسیر دسترسـی مهـاجمین بـه منـاطق حسـاس و کلیدی سیستم یا شبکه



امنیت سایبری



منشاء تهدیدات سایبری

منشاء انسانی:

- ✓ دولت‌های متخاصم
- ✓ مزدوران سایبری (گروه‌های تحت حمایت پنهان دولت های متخاصم)
- ✓ جاسوسان سایبری
- ✓ تروریست‌های سایبری
- ✓ مجرمین سازمان‌یافته سایبری
- ✓ هکرهای دارای انگیزه سیاسی
- ✓ ...

منشاء تجهیزاتی و سخت افزاری:

- ✓ تسلیحات سایبری
- ✓ بدافزارها (جاسوس‌افزارها، ویروس‌ها، کرم‌ها، هرزنامه‌ها و ...)
- ✓ سازه‌های مخرّب
- ✓ ...

شدت تهدیدات سایبری

شدت خیلی کم	تهدید سایبری تحت کنترل
شدت کم	تهدید سایبری حادثه آفرین
شدت متوسط	تهدید سایبری برهم زننده امنیت
شدت زیاد	تهدید سایبری بحران زا
شدت خیلی زیاد	تهدید سایبری فاجعه بار (مخل امنیت ملی)

سطح تهدیدات سایبری

فراملی : تهدید علیه فضای سایبر ی کشور و منافع کشور در فضای سایبری بین‌المللی

ملی : تهدید علیه کل یا بخش گسترده‌ای از فضای سایبری کشور

دستگاهی : تهدید علیه کل یا بخش قابل توجهی از یک زیرساخت در سطح ملی

استانی : تهدید علیه فضای سایبری یک استان کشور

منطقه حیاتی : تهدید علیه فضای سایبری یک منطقه حیاتی دارای اهمیت اقتصادی، سیاسی یا ...

زیرساختی : تهدید علیه فضای سایبری یک سازمان یا وزارتخانه

سطوح هشدار برای تهدیدات سایبری

احتمال وقوع / شدت پیامد	خیلی غیرمحتمل	غیرمحتمل	ممکن	محتمل	قریب‌الوقوع
خیلی کم (تحت کنترل)	۰	۱	۲	۳	٤
کم (حادثه آفرین)	۱	۲	۳	٤	٥
متوسط (مخلّ امنیت)	۲	۳	٤	٥	٦
زیاد (بحران‌زا)	۳	٤	٥	٦	۷
خیلی زیاد (فاجعه‌بار)	٤	٥	٦	۷	۸

۰ و ۱ و ۲	=	وضعیت سفید	=	تحت کنترل سایبری
۳ و ۴ و ۵	=	وضعیت زرد	=	تهدید سایبری
۶ و ۷	=	وضعیت نارنجی	=	بحران سایبری
۸	=	وضعیت قرمز	=	جنگ سایبری

سطوح هشدار برای تهدیدات سایبری

سطح هشدار	وضعیت سایبری	مفهوم	منشاء تهدید سایبری	پیامدهای تهدید سایبری	سطح تهدید سایبری	احتمال وقوع تهدید سایبری	شدت (پیامد) تهدید سایبری
٤	سفید	تحت کنترل سایبری	• جاسوسان صنعتی و اقتصادی • هکرها و Crackerها • خودی‌ها (هکرهای داخلی) • Phisherها • منتشرکنندگان هرزنامه	• نقض حریم خصوصی • نابودی یا تخریب محدود اطلاعات • ایجاد اختلال محدود در عملکرد سامانه‌ها و شبکه‌ها • دسترسی غیرمجاز به اطلاعات فاقد طبقه‌بندی و حساسیت • افشاء اطلاعات فاقد طبقه‌بندی • دستکاری (تغییر در) اطلاعات فاقد طبقه‌بندی • ممانعت از ارائه خدمات و انجام وظایف غیرحساس سایبری	• یک یا چند زیرساخت	• خیلی غیرمحتمل • غیرمحتمل • ممکن	• خیلی کم (رویداد) • کم (حادثه امنیتی کوچک) • متوسط (حادثه امنیتی عمده)

سطوح هشدار برای تهدیدات سایبری

سطح هشدار	وضعیت سایبری	مفهوم	منشاء تهدید سایبری	پیامدهای تهدید سایبری	سطح تهدید سایبری	احتمال وقوع تهدید سایبری	شدت (پیامد) تهدید سایبری
۳	زرد	تهدید سایبری یا اضطرار سایبری	• مجرمین سازمان-یافته سایبری • هکرهای دارای انگیزه سیاسی • متصدیان شبکه-های بات • نویسندگان جاسوس‌افزار و بدافزار	• نابودی یا تخریب عمده اطلاعات و یا تخریب اطلاعات دارای طبقه‌بندی • ایجاد اختلال گسترده در عملکرد سامانه‌ها و شبکه‌ها • دسترسی غیرمجاز به اطلاعات عمده و یا اطلاعات دارای طبقه‌بندی • افشاء اطلاعات عمده یا دارای طبقه‌بندی • دستکاری (تغییر در) اطلاعات عمده یا دارای طبقه‌بندی • ممانعت از ارائه خدمات و انجام وظایف حساس سایبری	• تعداد قابل توجهی زیرساخت • کلی یا بخش قابل توجهی از یک دستگاه • یک منطقه ویژه یا یک استان	• خیلی غیرمحتمل • غیرمحتمل • ممکن • محتمل • قریب‌الوقوع	• خیلی کم (رویداد) • کم (حادثه امنیتی کوچک) • متوسط (حادثه امنیتی عمده) • زیاد (بحران) • خیلی زیاد (فاجعه)

سطوح هشدار برای تهدیدات سایبری

سطح هشدار	وضعیت سایبری	مفهوم	منشاء تهدید سایبری	پیامدهای تهدید سایبری	سطح تهدید سایبری	احتمال وقوع تهدید سایبری	شدت (پیامد) تهدید سایبری
۲	نارنجی	بحران سایبری (مبارزه، ستیز، نزاع سایبری)	• مزدوران سایبری (گروه‌های تحت حمایت پنهان دولت‌ها) • جاسوسان سایبری • سرویس‌های امنیتی دولت‌ها • تروریست‌های سایبری	• صدمه به غرور ملی • ایجاد بحران منطقه‌ای • مخاطره منطقه‌ای برای سلامت و ایمنی عمومی • تخریب یا صدمه/ اختلال در سرمایه‌های ملی سایبری در حوزه منطقه‌ای • تخریب یا صدمه/ اختلال در اطمینان یا حساسیت‌های قومی • خسارت شدید اقتصادی	• تعداد زیادی زیرساخت • یک دستگاه • بیش از یک استان یا منطقه حیاتی	• ممکن • محتمل • قریب‌الوقوع	• متوسط (حادثه امنیتی عمده) • زیاد (بحران) • خیلی زیاد (فاجعه)

سطوح هشدار برای تهدیدات سایبری

سطح هشدار	وضعیت سایبری	مفهوم	منشاء تهدید سایبری	پیامدهای تهدید سایبری	سطح تهدید سایبری	احتمال وقوع تهدید سایبری	شدت (پیامد) تهدید سایبری
۱	قرمز	جنگ سایبری	• نیروهای نظامی کشور مهاجم (ارتش سایبری) یا سلاح‌های سایبری تحت کنترل یا رها شده توسط این نیروها	• براندازی نظام حاکمیتی یا تهدید فاجعه‌بار امنیت ملی • آغاز همزمان جنگ فیزیکی یا زمینه‌سازی و تسهیل شروع جنگ فیزیکی در آینده • تخریب یا صدمه فاجعه‌بار به وجهه کشور در سطح بین‌المللی • تخریب یا صدمه فاجعه‌بار به روابط سیاسی و اقتصادی کشور • تلفات انسانی یا مخاطره گسترده برای سلامت و ایمنی عمومی (از طریق ایجاد آلودگی هسته‌ای، شیمیایی یا بیولوژیک) • هرج‌ومرج و شورش داخلی • اختلال گسترده در اداره امور کشور • تخریب (یا صدمه گسترده به) اطمینان عمومی یا باورهای دینی، ملی و قومی • خسارت شدید به (یا اختلال گسترده در) اقتصاد ملی • تخریب یا اختلال گسترده در عملکرد زیرساخت‌ها	• حداقل دو دستگاه • چندین استان یا منطقه حیاتی • ملی • فراملی	• قریب‌الوقوع مطابق شرایط وضعیت	• خیلی زیاد (فاجعه)

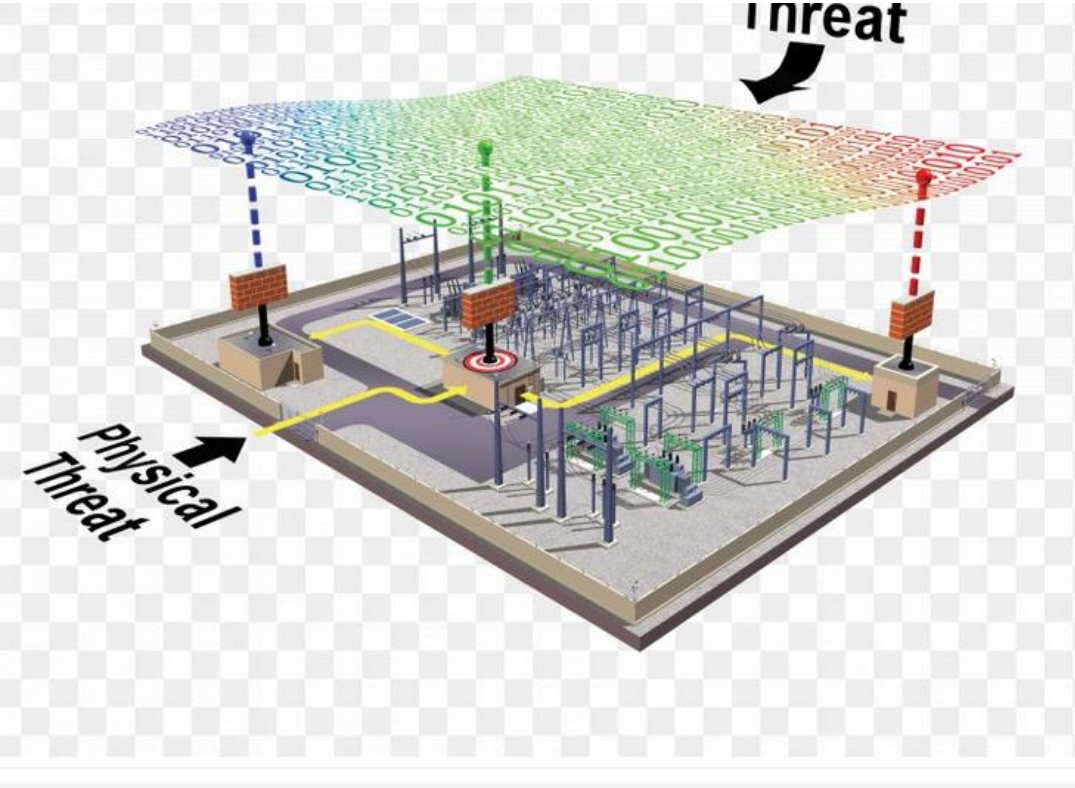
آسیب پذیری ها و مخاطرات فضای سایبر

آسیب پذیری های حوزه زیرساخت و شبکه:

- ضعف در طراحی و پیکربندی زیرساخت شبکه
- عدم یکپارچگی شبکه و زیرساخت
- عدم وجود UTM (شامل بسته های امنیتی کامل برای محافظت از شبکه و زیرساخت در مقابل تهدیداتی از جمله : ویروس ها، هرزنامه ها، بد افزار ها، برنامه های کلاه برداری، حملات امنیتی، نفوذ هکرها و ... می باشد. این بسته های امنیتی معمولاً شامل : فایروال، آنتی ویروس، آنتی اسپم، IPS و ... می باشند.

آسیب پذیری ها و مخاطرات فضای سایبر

آسیب پذیری های حوزه زیرساخت و شبکه:



- عدم وجود مراکز مانیتورینگ شبکه
- وجود شبکه های متعدد سازمانی
- آسیب پذیری شبکه های بی سیم
- عدم استفاده از Vlan

آسیب پذیری ها و مخاطرات فضای سایبر

آسیب پذیری های حوزه سرویس ها و سامانه ها:

- عدم یکپارچگی سرویس ها
- ضعف در طراحی منطقی و طراحی فیزیکی سامانه ها
- مشکلات موجود در زبان های برنامه نویسی
- مشکلات مربوط به عدم استفاده از SLC (Software Life Cycle)

آسیب پذیری ها و مخاطرات فضای سایبر

آسیب پذیری های حوزه سرویس ها و سامانه ها:

- ❑ حفره های موجود در سیستم عامل ها
- ❑ عدم بروزرسانی نرم افزارها
- ❑ نداشتن پیوست های فنی در تولید سامانه ها
- ❑ نداشتن پیوست امنیتی در بکارگیری سامانه ها

آسیب پذیری ها و مخاطرات فضای سایبر

آسیب پذیری های حوزه داده و اطلاعات :

- مشکلات نرمال سازی جداول داده در پایگاه های داده
- مشکلات مربوط به یکپارچگی و توزیع داده ها و بانک های اطلاعاتی
- مشکلات مربوط به BIG DATA
- ضعف در پروتکل های پشتیبان گیری
- ضعف در پروتکل های رمز

آسیب پذیری ها و مخاطرات فضای سایبر

آسیب پذیری های حوزه کاربران:

- آسیب پذیری های احراز هویت (کلمه عبور و .....)
- مشکلات دسترسی (RBAC و....)
- حملات phishing و ....

تعاریف

- با استقرار مرکز عملیات امنیتی در شبکه، پروسه حفاظت، ردیابی و عکس‌العمل در مقابل تهدیدات امنیتی در یک سازمان در اختیار **SOC** قرار می گیرد.

- پس از استقرار این مرکز هر یک میلیون رویداد بطور معمول بر اساس پاسخگویی خودکار و برخوردهای هوشمند مبتنی بر یک سیستم خبره، به کمتر از ۱۰ مورد برای بازبینی مدیر یا راهبر شبکه کاهش خواهد یافت.

مزایای SOC

- کاهش زمان قطعی شبکه و هزینه های آن
- کنترل تهدیدات امنیتی و جلوگیری از وقوع حملات امنیتی و کاهش هزینه های راهبری شبکه
- کاهش نیاز به پرسنل فنی متخصص در امر امنیت شبکه
- تخفیف صدمات وارده ناشی از انواع حملات امنیتی به شبکه
- واکنش سریع در مقابل حملات امنیتی و بازیابی اطلاعات
- استفاده بهینه از ابزارهای امنیتی شبکه

بخش های مرکز عملیات

۱- سیستم جمع آوری لاگ

مسئولیت جمع آوری لاگ های تجهیزات مختلفی مانند فایروال ها، روترها، سوییچ ها، سرورها و سرویس های حساس سازمان و نیز نرم افزارها و سیستم های اطلاعاتی مهم و کلیدی سازمان را بر عهده داشته و بخشی از اطلاعات اولیه خود را از سیستم های تشخیص نفوذ، آنتی ویروس ها، سیستم پایش گردش کار، پایش گردش محتوا و میزبان ها به دست می آورد. در حقیقت این سیستم مسئولیت جمع آوری داده های خام اولیه جهت تحلیل توسط واحد سیستم مدیریت رویداد را بر عهده دارد.

بخش های مرکز عملیات

۲- سیستم مدیریت رویداد

سیستم مدیریت رویداد، مسئولیت شناسایی رویدادها را با توجه به وقایع شناسایی شده توسط سیستم مدیریت لاگ و نیز با توجه به گزارش های دریافتی از مدیران سیستم ها، مدیران شبکه و متخصصین امنیت، برعهده دارد و رویدادهای شناسایی شده را در جهت تشخیص تهدید به واحد مدیریت تهدیدها ارسال می کند.

بخش های مرکز عملیات

۳- سیستم مدیریت تهدیدات

بعد از شناسایی رویداد توسط سامانه مدیریت رویداد، سیستم مدیریت تهدیدات، باید آسیب پذیری ها و تهدیدهای مرتبط با هر رویداد را شناسایی کند، به این منظور در مرحله اول، سیستم باید پایگاه داده خود را بررسی کرده و در صورت عدم تشخیص تهدید و آسیب پذیری مربوط به هر رویداد، سیستم باید قابلیت ارتباط با پایگاه داده های آسیب پذیری بیرونی را نیز داشته باشد و اقدام به شناسایی تهدیدها و عامل آسیب پذیری که منجر به بروز رویداد شده است، شود.

معماری SOC

- هر مرکز عملیات امنیتی از پنج مؤلفه اصلی تشکیل شده است : مولد رویدادها، جمع کننده رویدادها، پایگاه داده پیام ها، موتور تحلیل و نرم افزار مدیریت واکنش ها

جعبه : E مولد رویدادها

جعبه: D پایگاه داده رویدادها

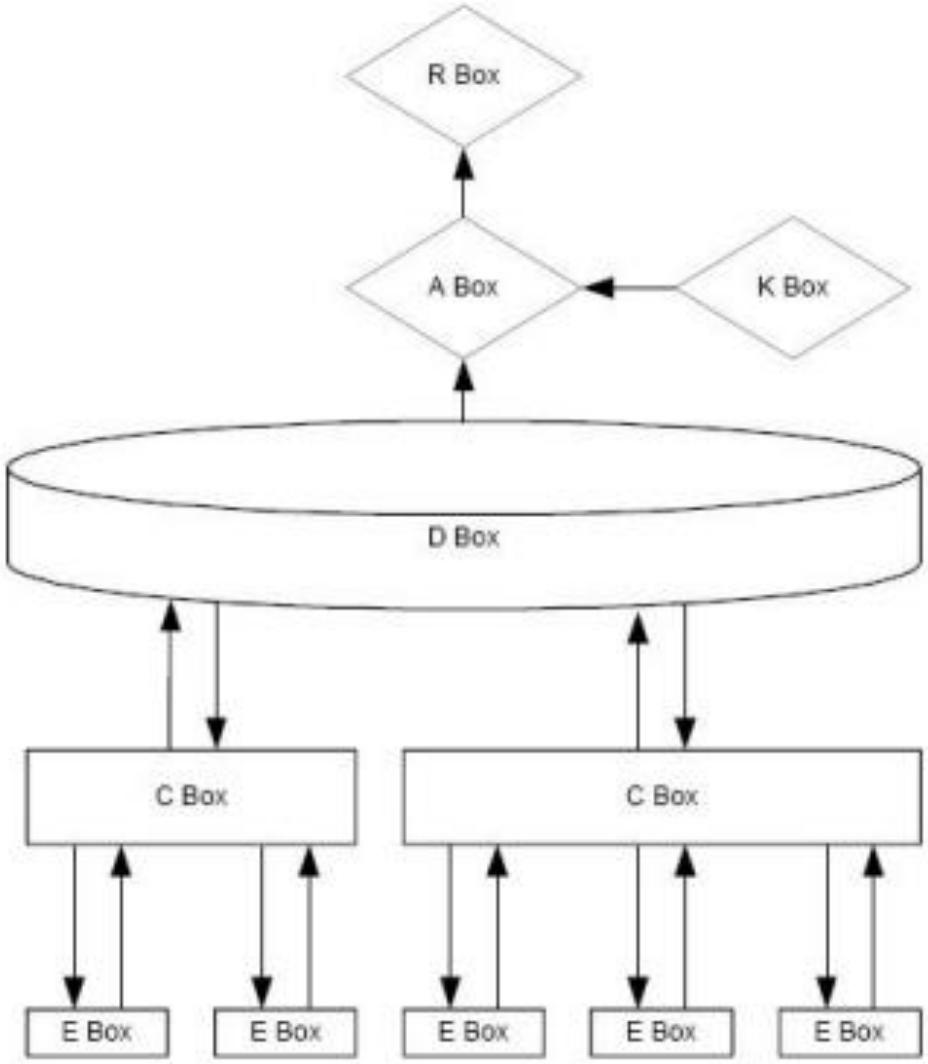
جعبه : R سیستم واکنش به رویدادها

جعبه: A سیستم تحلیل رویدادها

جعبه: C سیستم جمع کننده و فرم دهنده رویدادها

جعبه: K پایگاه دانش

معماری SOC



R Box
reaction and reporting

A Box + **K Box**
incident analysis — knowledge base

D Box
formated messages database

C Boxes
collection boxes

E Boxes
event generators : sensors & pollers

لزوم بومی بودن SOC

- استفاده از ابزارهای امنیتی بومی در بخشهای مختلف.
- استفاده از نیروی متخصص داخلی و پشتیبانی فنی شبانه روزی توسط متخصصین امنیتی.
- امکان انواع پیاده سازی بصورت تمام برون سپاری، نیمه برون سپاری و درون سازمانی بسته به سیاست سازمان مربوطه.
- امکان ارائه آموزش های فنی خاص به مدیران و راهبران شبکه.
- تدوین رویه ها، سازوکارها و سیاست های امنیتی بر اساس استانداردهای بومی

مشخصات یک SOC بومی

- قابلیت اطمینان بالای سیستم با انجام پشتیبان گیری منظم، استفاده از ابزارهای امنیتی پشتیبان و منابع تغذیه مناسب.
- قابلیت نگهداری و پردازش حجم بالای رویدادهای امنیتی شبکه و ارائه گزارش های منظم
- قابلیت توسعه سیستم
- پشتیبانی از انواع زیرساخت های شبکه

تعاریف

سیستم مدیریت امنیت اطلاعات (ISMS) راهکار حل مشکلات امنیتی در سیستم‌های اطلاعاتی است، یک سیستم جامع امنیتی که بر سه پایه بنا شده است:

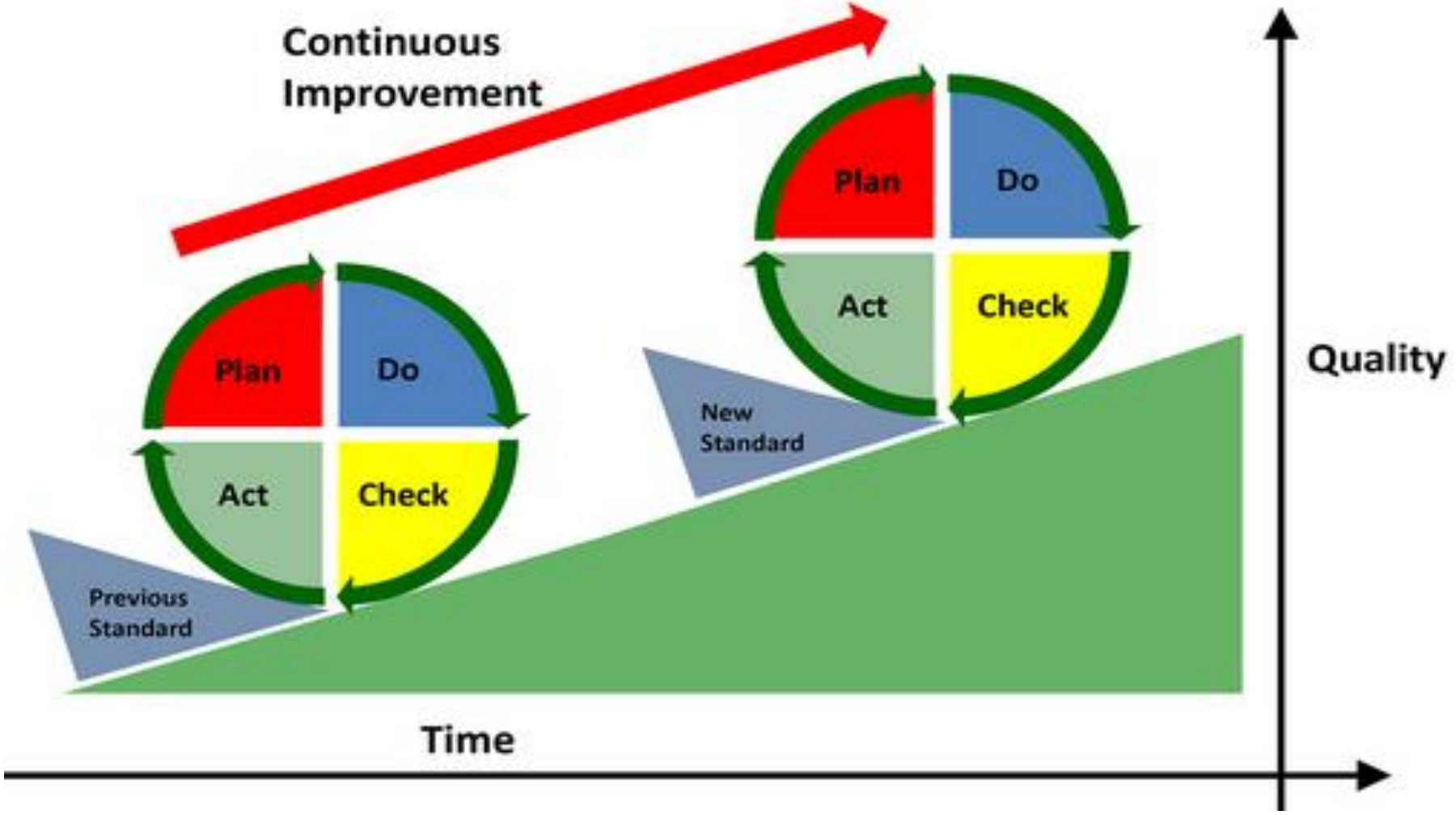
- بررسی و تحلیل سامانه های اطلاعاتی
- سیاست ها و دستورالعمل های امنیتی
- فناوری و محصولات امنیت

ISMS: Information Security Management System

تعاریف

با ارائه اولین استاندارد مدیریت امنیت اطلاعات در سال 1995، نگرش سیستماتیک به مقوله ایمن‌سازی فضای تبادل اطلاعات شکل گرفت. بر اساس این نگرش، تامین امنیت فضای تبادل اطلاعات سازمان ها، دفعتا مقدور نمی‌باشد و لازم است این امر به صورت مداوم در یک چرخه ایمن‌سازی شامل مراحل طراحی، پیاده‌سازی، ارزیابی و اصلاح، انجام گیرد.

تعاریف


Continuous
Improvement
Plan
Do
Act
Check
Plan
Do
Act
Check
New
Standard
Previous
Standard
Quality
Time

:PLAN

این فاز در واقع مرحله مشخص شدن تعاریف اولیه پیاده سازی ISMS میباشد.تهیه سیاست های امنیتی، مقاصد،تعریف پردازش های مختلف درون سازمانی و روتین های عملیاتی و غیره در این مرحله تعریف و پیاده سازی می شوند.

:DO

پیاده سازی و اجرای سیاست های امنیتی،کنترل ها پردازش ها در این مرحله انجام می شود.

:CHECK

در این مرحله ارزیابی موفقیت پیاده سازی سیاست های مختلف امنیتی،همچنین تجربه های عملی و گزارش های مدیریتی گرد آوری خواهند شد.

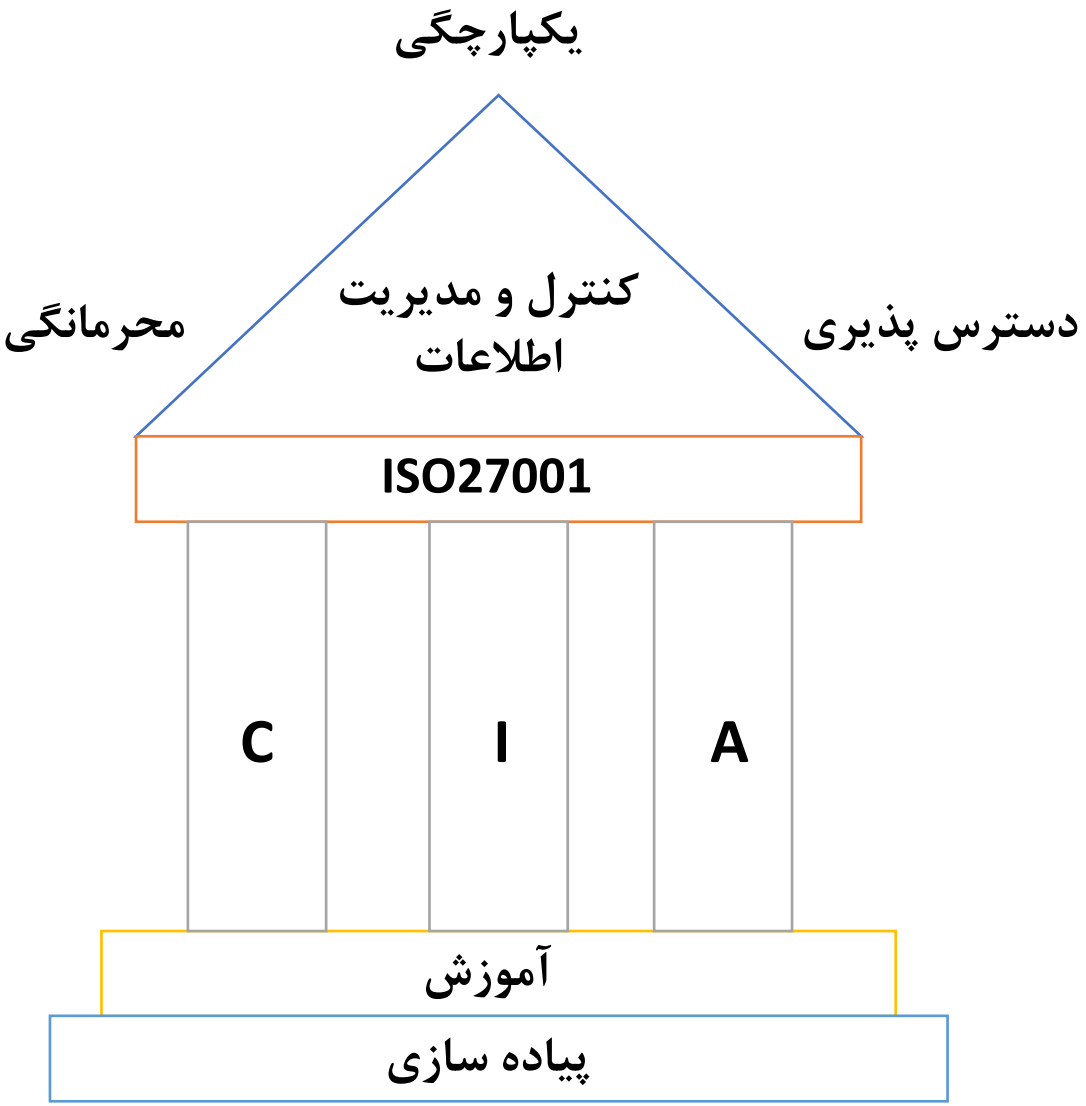
:ACT

اجرای موارد ترمیمی و بازنگری در نحوه مدیریت اطلاعات، همچنین تصحیح موارد مختلف در این فاز انجام می شود.

در هر چرخه موارد زیر لحاظ شده است:

- ❑ تعیین مراحل ایمن‌سازی و نحوه شکل‌گیری چرخه امنیت اطلاعات و ارتباطات سازمان
- ❑ جزئیات مراحل ایمن‌سازی و تکنیک های فنی مورد استفاده در هر مرحله
- ❑ لیست و محتوای طرح‌ها و برنامه‌های امنیتی مورد نیاز سازمان
- ❑ ضرورت و جزئیات ایجاد تشکیلات سیاستگذاری، اجرائی و فنی تامین امنیت اطلاعات و ارتباطات سازمان
- ❑ تعیین کنترل‌های امنیتی مورد نیاز برای هر یک از سیستم‌های اطلاعاتی و ارتباطی سازمان

امنیت سایبری



علل بروز مشکلات امنیتی

- ضعف فناوری
- ضعف پیکربندی
- ضعف سیاست ها

ضعف فناوری

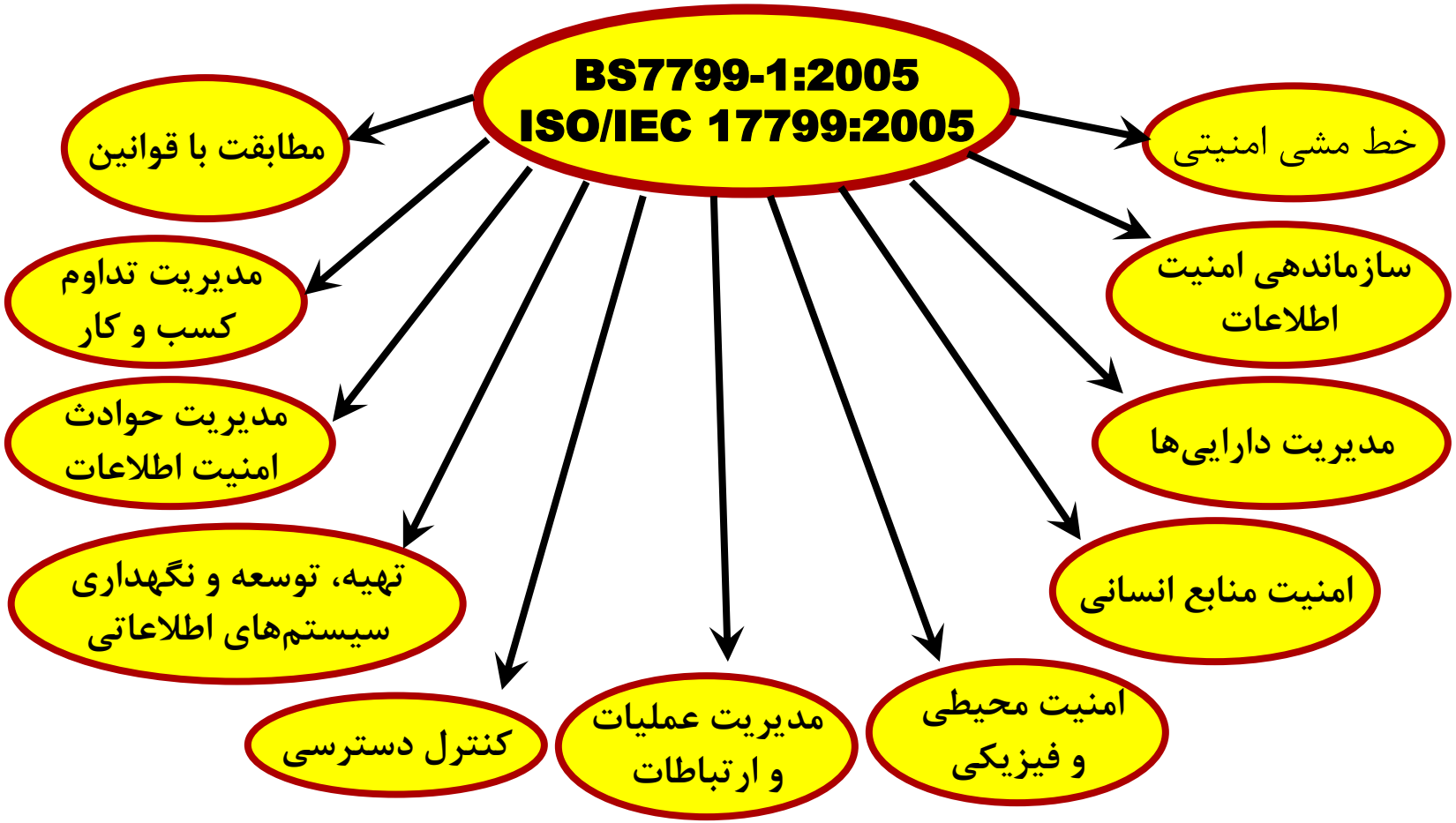
- ✓ ضعف پروتکل ها: TCP/IP
- ✓ ضعف سیستم عامل
- ✓ ضعف تجهیزات شبکه ای

ضعف پیکربندی

- ✓ استفاده غیرایمن از account کاربران
- ✓ استفاده از system account که رمز عبور آنها به سادگی قابل تشخیص است.
- ✓ عدم پیکربندی صحیح سرویس های اینترنت
- ✓ غیر ایمن بودن تنظیمات پیش فرض در برخی محصولات
- ✓ عدم پیکربندی صحیح تجهیزات شبکه ای

ضعف سیاست ها

- ✓ عدم وجود یک سیاست امنیتی مصوب
- ✓ رها کردن مدیریت امنیت شبکه به حال خود
- ✓ نصب و انجام تغییرات مغایر با سیاست های تعریف شده
- ✓ عدم وجود برنامه ای مدون جهت برخورد با حوادث غیرمترقبه


BS7799-1:2005
ISO/IEC 17799:2005
مطابقت با قوانین
خط مشی امنیتی
مدیریت تداوم کسب و کار
سازماندهی امنیت اطلاعات
مدیریت حوادث امنیت اطلاعات
مدیریت دارایی‌ها
تهیه، توسعه و نگهداری سیستم‌های اطلاعاتی
امنیت منابع انسانی
کنترل دسترسی
مدیریت عملیات و ارتباطات
امنیت محیطی و فیزیکی

حوزه اول: خط مشی امنیتی

هدف: جهت‌گیری و حمایت مدیریت سازمان در خصوص تامین نیازمندی‌ها و مقررات امنیت اطلاعات

- مستند خط مشی امنیت اطلاعات سازمان
- بازنگری خط مشی امنیت اطلاعات سازمان

حوزه دوم: سازماندهی امنیت اطلاعات

هدف: سازماندهی مدیریت امنیت اطلاعات در داخل سازمان

- ایجاد هماهنگی بین واحدهای تامین امنیت اطلاعات
- تعیین و تخصیص مسئولیت‌های مرتبطین با امنیت اطلاعات
- فرآیندهای مجاز برای پردازش اطلاعات
- توافقنامه محرمانگی اطلاعات سازمان

حوزه سوم: مدیریت دارایی‌ها

هدف: تامین و تداوم محافظت‌های مناسب برای سرمایه‌های سازمان

- تهیه فهرست از سرمایه‌های سازمان
- ارزش‌گذاری سرمایه‌های سازمان
- استفاده صحیح از سرمایه‌های سازمان
- تدوین راهنمای طبقه‌بندی اطلاعات
- نشانه‌گذاری و پشتیبانی از اطلاعات

حوزه چهارم: امنیت منابع انسانی

اهداف:

۱- اطمینان از اطلاع کارکنان از مسئولیت‌هایشان و متناسب بودن صلاحیت افراد برای انجام وظایف

۲- اطمینان از اینکه کارکنان و کاربران از تهدیدهای امنیت اطلاعات و اهمیت آنها اطلاع دارند.

- وظایف و مسئولیت‌ها
- بررسی صلاحیت
- تعیین مدت و شرایط همکار کارکنان
- مسئولیت مدیران
- آگاهی رسانی، کسب مهارت و آموزش امنیت اطلاعات
- فرآیندهای انضباطی

حوزه چهارم: امنیت منابع انسانی

اهداف

۳- اطمینان از شیوه مناسب خاتمه دادن به همکاری کارکنان، طرف‌های قرارداد در زمان خاتمه

- تعریف و ابلاغ شفاف مسئولیت‌های کارکنان در زمان خاتمه همکاری یا جابجایی در سازمان
- مسئولیت کارکنان، طرف‌های قرارداد و کاربران در خصوص بازگرداندن سرمایه‌های سازمان در زمان خاتمه همکاری، قرارداد یا موافقت‌نامه
- حذف مجوزهای دسترسی کارکنان، طرف‌های قرارداد و کاربران، در زمان خاتمه همکاری یا جابجایی در داخل سازمان

حوزه پنجم: امنیت فیزیکی و محیطی

هدف: جلوگیری از دسترسی فیزیکی غیر مجاز، خسارت و توقف فعالیت‌های سازمان

- ایجاد محیط امن، به ویژه برای اطلاعات و سیستم‌های اطلاعاتی
- کنترل تردد فیزیکی
- امن‌سازی دفاتر، اتاق‌ها و امکانات
- جداسازی فضاهای دسترسی عمومی

حوزه ششم: مدیریت عملیات و ارتباطات

هدف: تشخیص فعالیت های غیر مجاز پردازش اطلاعات

- نظارت بر ثبت وقایع
- استفاده از سیستم‌های مانیتورینگ
- محافظت از اطلاعات ثبت وقایع
- ثبت عملکرد مدیران و اپراتورهای سیستم‌ها
- ثبت خطاها
- هم‌زمان نمودن ساعت سیستم‌ها

حوزه هفتم: کنترل دسترسی

اهداف

۱- کنترل دسترسی به اطلاعات

۲- اطمینان از دسترسی کاربران مجاز و پیش‌گیری از دسترسی غیر مجاز به اطلاعات و سیستم‌ها

۳- پیش‌گیری از دسترسی کاربران غیر مجاز به اطلاعات و سیستم‌ها و دزدی اطلاعات

۴- پیش‌گیری از دسترسی غیر مجاز به سرویس‌های شبکه

۵- پیش‌گیری از دسترسی غیر مجاز به سیستم عامل‌ها

۶- پیش‌گیری از دسترسی غیر مجاز به اطلاعات داخل سیستم‌های اطلاعاتی

۷- اطمینان از امنیت اطلاعات در زمان استفاده از کامپیوترهای قابل حمل

حوزه هشتم: تهیه، توسعه و نگهداری سیستم‌ها

اهداف:
۱) تامین محرمانگی، اصالت و صحت اطلاعات با استفاده از مکانیزم های رمزنگاری
۲) اطمینان از امنیت فایل سیستم نرم‌افزارهای کاربردی
۳) تامین تداوم امنیت اطلاعات و سیستم‌های عملیاتی
۴) کاهش مخاطرات ناشی از بهره‌برداری از آسیب‌پذیری‌های فنی منتشر شده

- **سیاست استفاده از کنترل‌های رمزنگاری**
- **مدیریت کلید (به منظور استفاده از رمزنگاری)**
- **کنترل نرم‌افزارهای عملیاتی**
- **حفاظت از سیستم تست داده‌ها**
- **کنترل دسترسی به source برنامه‌ها**

حوزه نهم: مدیریت حوادث امنیتی

اهداف
۱) اطمینان از گزارش به موقع حوادث و ضعف‌های سیستم‌های اطلاعاتی
۲) اطمینان از اعمال رویه‌های یکنواخت و موثر در مورد حوادث امنیتی

- گزارش حوادث امنیت اطلاعات
- گزارش ضعف‌ها و آسیب‌پذیری‌های امنیتی
- مسئولیت‌ها و رویه‌ها
- یادگیری (تجربه اندوزی) از حوادث امنیتی گذشته
- جمع آوری شاهد و مدارک

حوزه دهم: مدیریت تداوم کسب و کار

هدف: خنثی‌سازی وقفه در فعالیت‌های تجاری سازمان و محافظت از فرآیندهای تجاری حساس سازمان از تاثیر صدمه به سیستم‌های اطلاعاتی یا حوادث و اطمنیان از فعال شدن مجدد سیستم‌ها

- توجه به امنیت اطلاعات در فرآیند مدیریت کسب و کار سازمان
- تدوام و کسب و کار ارزیابی مخاطرات
- توسعه و پیاده‌سازی طرح‌های تداوم کسب و کار با در نظر گرفتن امنیت اطلاعات
- چارچوب طرح تداوم کسب و کار
- تست، نگهداری و ارزیابی مجدد طرح‌های تداوم کسب و کار

حوزه یازدهم: سازگاری با قوانین

اهداف:
۱) اجتناب از نقض قوانین، مقررات، مسئولیت‌های قراردادی و نیازمندی‌های امنیتی
۲) اطمینان از سازگاری سیستم‌ها با سیاست‌ها و استانداردهای امنیتی سازمان

- سازگاری با سیاست‌ها واستانداردهای امنیتی
- شناسایی قوانین مرتبط
- محافظت از اطلاعات و حریم خصوصی کارکنان
- پیش‌گیری از سوء استفاده از امکانات پردازش اطلاعات
- تنظیم ضوابط کنترل‌های رمزنگاری
- بررسی سازگاری فنی

با تشکر