دانشگاه آزاد اسلامی
واحد تهران مرکز – دانشکده مدیریت
کارشناسی ارشد مدیریت فن آوری اطلاعات
درس : تاثیر فناوری اطلاعات بر سازمان

# نقش فناوری اطلاعات در کنترل

استاد : جناب آقای دکتر احمدی بافنده

ارائه‌کنندگان : آمنه اشراقی – زهرا یاوری

نیمسال اول تحصیلی ۹۴-۱۳۹۳

# فهرست

# مفهوم کنترل

- نظـارت و کنتـرل یکـي از اجـزاي اصـلي مـديريت محسـوب مي‌گردد به طوري که بدون توجه به اين جز ساير اجزا مـديريت، از قبيـل برنامـه‌ريزي، سـازماندهي و هـدايت نيـز نـاقص بـوده و تضميني براي انجام درست آنها وجود ندارد.

- مي‌توان کنترل را پشتوانه تحقق هـدف‌هاي سـازمانی و اجـرای درسـت تصميم‌هاي به‌موقع دانست.

# هدف کنترل

- هدف از انجام کنترل و نظارت عبارت است از این که مشخص گردد آیا سازمان یا مؤسسه به اهداف خود نایل آمده است یا خیر؟ و اگر اهداف محقق شده‌است تحقق اهداف به چه میزان است.



# ضرورت کنترل درسازمان‌ها

- هـدف و فلسـفه وجـودي نظـارت و کنتـرل اصـلاح و بهبـود اسـت و اگـر ايـن ويژگـــي در نظـــام کنترلـــي موجـــود نباشـــد، سيســـتم دوام چنـــداني نخواهدداشت. نهادهاي نظارتي بايد تلاش کنند تا پس از شناسايي دقيـق مشـکلات و موانـع، آنهـا را ريشـه‌يابي کـرده و را ەحلهـاي اصـلاحي را ارائـه نمايند.
- هدف نهايي هر نظام کنتـرل و نظـارت بـالا بـردن سـطح کـارايي و در نتيجـه ميزان توليد و ارائه خدمات بهينه به مشتريان مي‌باشد.

# طراحي سيستم كنترل

- یکی از وظایف اصلی مدیر طراحی سیستم کنترل در سازمان است. برای طراحی این سیستم معمولاً طی مراحل زیر ضروری است:

**۱) تعیین نتایج مورد انتظار (بایدها) در کنترل**

در این مرحله مدیریت باید اهداف و نتایجی را که از اجرای برنامه‌ها انتظار دارد مشخص‌سازد.

**۲) تعیین شاخص برای سنجش نتایج مورد انتظار**

این شاخص‌ها مقیاس‌هایی برای سنجش عملکردها بشمار می‌روند و در جریان کنترل باید شاخص‌هایي وجود داشته‌باشد تا بتوان به وسیله آنها میزان نیل به نتایج را مورد سنجش قرار داد.

# طراحي سيستم كنترل

**۳) تعیین استاندارد یا الگوی مطلوب**

پس از آنکه شاخص‌ها یا مقیاس‌های سنجش مشخص شدند باید میزان مورد نظر در آن شاخص‌ها برای موضوع کنترل تعیین شود. استانداردها خود به صورت زیر تدوین می شوند:

**۳-۱) استانداردهای تاریخی:** این نوع استانداردها بر اساس تجربیات و اطلاعات گذشته بدست می‌آیند.

**۳-۲) استانداردهای تطبیقی یا خارجی:** این نوع استانداردها از سایر سازمان‌ها و واحدهای مشابه اقتباس می‌شود.

**۳-۳) استانداردهای مهندسی یا کارسنجی:** این نوع استانداردها از طرق مختلف (مطالعه کار) بدست می‌آیند.

**۳-۴) استانداردهای نظری:** قضاوت ذهنی مدیران و صاحب‌نظران، پدیدآورنده این نوع از استانداردها هستند.

# طراحي سيستم كنترل

**۴) طراحی شبکه اطلاعاتی در کنترل**

در طراحی شبکه اطلاعاتی باید به این نکته توجه داشت که اطلاعات اضافی به همان اندازه مشکل آفرینند که اطلاعات ناقص مسئله ساز هستند. همچنین شبکه اطلاعاتی باید بتواند اطلاعات را بطور مستمر به روز درآورده و آخرین اطلاعات را در اختیار مسئولان مربوطه قرار دهد.

**۵) ارزیابی اطلاعات و نتیجه گیری**

در این مرحله به کمک استانداردهای انتخابی، اطلاعات جمع‌آوری شده مورد ارزیابی قرار می‌گیرند.

# مشخصات سیستم کنترل مؤثر

- **مشخصات سیستم کنترل مؤثر**

اصولاً سیستم‌های کنترل باید با توجه به مقتضیات سازمان طراحی شده و در هر مورد ویژگی‌های مربوط به آن را دارا باشند. این خصوصیات شامل موارد زیر هستند:

- ✓ کنترل باید اقتصادی باشد به طوری که نتایج آن بر هزینه‌های آن فزونی یابد.
  ـ نتیجه کنترل > هزینه کنترل
- ✓ در اعمال کنترل‌ها نباید افراط و تفریط شود.
- ✓ کنترل‌ها باید در نقاط حساس و کلیدی باشند.
- ✓ کنترل‌ها باید متناسب با برنامه و فعالیت‌ها تنظیم شوند.
- ✓ سیستم کنترل باید به نحوی طراحی شوند که اطلاعات و نتایج کنترل در سریع‌ترین زمان ممکن در اختیار مسئولین قرار گیرد.

# مشخصات سیستم کنترل مؤثر

- کنترل باید عینیت داشته باشد و صرفاً بر اساس ذهنیات و نظرات اشخاص نباشد.
- کنترل‌ها باید واقع‌بینانه باشند.
- سیستم کنترل باید انعطاف لازم را داشته باشد.
- کنترل باید وسیله اصلاح باشد نه تنبیه و مجازات.
- سیستم کنترل باید با فرهنگ سازمان تناسب داشته‌باشد.
- کنترل نباید فقط بر نقاط ضعف تأکید ورزد و باید نقاط قوت را نیز در نظر گیرد.
- مسئولین و متولیان امر کنترل باید واجد صلاحیت باشند.
- سیستم کنترل باید دقیقاً مشخص سازد که نتایج کنترل در اختیار چه کسانی قرارگیرد.

# نقش ابزار فناوري اطلاعات در کنترل

- بی‌شک امروزه و با توجه به مطرح‌شدن مسائلی چون سازمان‌های الکترونیکی که مفاهیم الکترونیکی متعددی در همه امور مانند، شهر الکترونیک، دولت الکترونیک، شهروند الکترونیک، بانکداری الکترونیک، سلامت الکترونیک و ... را ایجاد کرده‌اند، وابستگی سازمان‌ها، کارکنان و مراجعه‌کنندگان به ابزاری با نام فناوری اطلاعات افزایشی چشم‌گیر یافته‌است، چنانچه که اگر به هر ترتیبی از این ابزار استفاده‌نشده یا در روند استفاده از این تکنولوژی خللی ایجادشود، انواع و اقسام تعاملات سازمانی دستخوش نقصان و خطر خواهندشد.

# نقش ابزار فناوري اطلاعات در كنترل

- امروزه فناوري اطلاعات يك عامل تسهيل‌كننده اصلي در فعاليت‌هاي كسب و كار سازمان‌هاست.
- از اين رو به كارگيری فناوري اطلاعات، يك مزيت سازمانی است و به منظور كسب موفقيت، سازمان‌ها لازم است به گونه مؤثر دراستفاده از فرصت‌ها و تهديدهاي مربوط به آن، مديريت شوند.



# نقش ابزار فناوري اطلاعات در كنترل

- در کشورهای توسعه‌یافته ، تحقیقات و مدیریت فناوری‌های جدید از جمله تحقیقات و مدیریت فناوری اطلاعات مورد توجه جدی می‌باشد .
- به نحوی که در اکثر موارد مراکز تحقیقاتی مستقل فناوری اطلاعات و همچنین وزارتخانه‌ای با عنوان وزارت فناوری اطلاعات در کنار وزارتخانه‌های دیگر سکان امور فناوری اطلاعات آن کشور را عهده‌دار می‌باشد.
- شاید یکی از دلائل اصلی پیشرفت و موفقیت آن کشورها در مقوله توسعه فناوری اطلاعات و ارتباطات در کشورشان توجه جدی به این مقوله بوده‌است.

# نقش ابزار فناوري اطلاعات در کنترل

- بدیهی است که تصمیم‌گیری به شیوه‌ای کارآمد، به خصوص در دنیای پیچیده کنونی، مستلزم به کارگیری و برخورداری از مقادیر زیادی از اطلاعات می‌باشد.
- در واقع اطلاعات به عنوان ابزاری راهبردی، رکنی مهم در تصمیم‌سازی مدیریت محسوب می‌شود. بی‌شک اتخاذ روش یک مدیر برای تصمیم‌گیری، بستگی به صحت و دقت اطلاعاتی دارد که در زمان تصمیم‌گیری، در اختیار وی قرار دارد.
- البته کاملا واضح است که به منظور جمع‌آوری داده‌های اولیه که به دست پردازش سپرده خواهند شد، وجود یک سیستم کارآمد نظارتی بسیار ضروری است.

# نقش ابزار فناوري اطلاعات در کنترل

- شـرکت‌های مجهـز بـه ابزارهـای فنـاوری اطلاعـات و ارتباطـات، می‌تواننـد اطلاعات مربوط به واحدهای مختلف خـود را بـه صـورت سـاده در مـدت زمـانی بسـیار کوتاه به پایگاه داده مرکزی انتقال دهند و سـپس به وسـیله نرم‌افزارهای کاربردی ویژه به سـرعت دسـته‌بندی و تجزیـه و تحلیـل کننـد و در اختیـار افـراد مورد نظر قراردهند، یا به صـورت پیچیـده‌تر بـا اسـتفاده از **ERP** اطلاعـات داخـل سازمانی را مدیریت کنند.

- **سیسـتم جـامع نـرم افـزاری کـه بـه کمک آن می تـوان تمـام فعالیتهـای اطلاعـاتی سـازمان را یکپارچـه و منـابع سـازمانی (پـول، نیـروی انسـانی، کـالا، تجهیـزات) را بـا هـدف افزایش بهره وری، برنامه ریزی و مدیریت کرد)** ***Enterprise Resorurce Planning*** **:**

# نقش ابزار فناوري اطلاعات در کنترل

- **از جمله دستاوردهای ERP می توان به موارد زیر اشاره کرد:**

- ✓ برقراری فرایندگرایی به جای وظیفه‌گرایی در سازمان
- ✓ نظام مندکردن چگونگی انجام فرآیندهای کاری
- ✓ کمک در دستیابی به مزایای رقابتی از راه بهبود فرآیندها
- ✓ توانایی هماهنگی سریع با تغییر شرایط برون سازمانی – تجارت الکترونیکی
- ✓ توانایی هماهنگ‌کردن سیستم سازمان با تکنولوژی‌های روز: وب، اینترنت و ...
- ✓ توسعه زیرساخت لازم به منظور وارد شدن به بحث کسب و کار الکترونیکی
- ✓ امکان و یا تسهیل توسعه سیستم‌ها و تکنولوژی‌های جدید از جمله تولید بهنگام
- ✓ ایجاد یکپارچگی سازمانی از بعد اطلاعاتی و افزایش سازگاری در اطلاعات سازمانی
- ✓ ارتباط مستمر با تأمین‌کنندگان، توزیع‌کنندگان و مشتریان

# نقش ابزار فناوري اطلاعات در کنترل

- امروزه فناوری اطلاعات این امکان را به وجود آورده‌است تا چندین عضو یک گروه با استفاده از رایانه‌های شخصی خود در مناطق مختلف دنیا، تشکیل جلسه داده، به صورت گروهی تصمیم‌گرفته، برنامه‌ریزی‌کنند.
- به عبارت دیگر زمینه برای مشارکت بیشتر و مستقیم کارکنان و به ویژه مدیران رده میانی در تصمیم‌های مربوط به هدف‌ها، استراتژی‌ها و برنامه‌های سازمان فراهم شده‌است.

# نقش ابزار فناوري اطلاعات در کنترل

- گستردگی تحولات و دگرگونی‌های داخلی و خارجی سازمان‌ها، ضرورت اخذ تصمیمات پیچیده‌تر را برای مدیران آشکار ساخته‌است، بطوری که در حال حاضر، بدون دسترسی به سیستم‌های اطلاعاتی مدیریت، تصمیم‌گیری به مفهوم علمی آن ممکن نمی‌باشد.
- یکی از متفکران عرصه مدیریت، عدم اطمینان و پیش‌بینی‌ناپذیری امور و تحولات را از بارزترین ویژگی‌های انتقال از محیط های ساده به پیچیده یا محیطهای ایستا به پویا و اتخاذ تصمیمات برنامه‌ریزی نشده می‌داند.
- حال آنکه به علت تراکم امور جاری و گستردگی شاخه‌های عملیاتی، یکی از روش‌های ایجاد یک نظارت کارآمد در امور اجرایی، استفاده از روش‌های رایانه‌ای و اتوماتیک نمودن امور کنترل در بازوهای اجرایی است.

# نقش ابزار فناوري اطلاعات در کنترل

- امروزه به کمک ICT امکان کنکاش، بررسی و پیگیری عوامل محیطی بسیار سریعتر و ارزانتر از گذشته فراهم آمده‌است.
- (Information and Communication Technologies: فن آوری اطلاعات و ارتباطات: به مجموعه امکانات سخت افزاری، نرم افزاری، شبکه ای و ارتباطی به منظور دستیابی مطلوب به اطلاعات، گفته می شود)
- در نتیجه هر سازمانی برای کسب اطلاعات لازم درباره عوامل محیطی برای ارزیابی میزان درستی و دقت پیش‌فرضهای خود درباره محیط می‌تواند بسیار راحت‌تر و کم‌هزینه‌تر از گذشته عمل کند. به علاوه محدودیت زمانی نیز وجود ندارد، یعنی در هر ساعتی از شبانه‌روز می‌تواند به این اطلاعات دسترسی پیداکند.

# نقش ابزار فناوري اطلاعات در کنترل

- با توسعه فناوری اطلاعات، پردازش داده‌ها در مقیاس وسیع و تجزیه و تحلیل آن‌ها در زمان بسیار کوتاه و با صرف هزینه‌های ناچیز امکان‌پذیرشده‌است.
- بنابراین مدیران با استفاده از این منابع اطلاعاتی می‌توانند از یک سو به تجزیه و تحلیل روندهای محیطی بپردازند و از سوی دیگر به سنجش دقیق عملکردها و مقایسه دستاوردها با هدف‌های برنامه‌ها مبادرت ورزند و هرگونه انحراف را به سرعت شناسایی کرده و در زمان مناسب مورد رسیدگی قراردهند.

# نقش ابزار فناوري اطلاعات در كنترل

- یکی از ابزارهای فناوری اطلاعات عبارت از سیستم اطلاعاتی مدیران اجرایی یا **EIS** (Executive Information System) است.
- در واقع **EIS** سیستم‌های مدیریتی‌اند که برای اطلاعات استراتژیک مدیران سطح بالای سازمان طراحی می‌شوند. هدف آنها پشتیبانی مدیران با دسترسی آسان و فوری به اطلاعات کلیدی مورد نظرشان برای رسیدن به هدف‌های شرکت است.
- یکی دیگر از سیستم‌های مبتنی بر فناوری اطلاعات و ارتباطات که در این زمینه مورد استفاده قرار می‌گیرید، سیستم اطلاعات استراتژیک **SIS** (Strategic Information System) است که می‌تواند جریان اطلاعات استراتژیک را توسعه و بهبود بخشد.

# نقش ابزار فناوري اطلاعات در کنترل

- مـدیران در صـورت اسـتفاده از تجهیـزات فنـاوری اطلاعـات و در اختیار داشتن پروسه‌هـای عملیـاتی و بایـدها و نبایـدهایی کـه توسـط سیاسـتگزاران اولیـه تهیـه شده‌اسـت، مـی‌تواننـد بـا اسـتفاده از سیسـتم‌هـای انفورماتیـک و داده‌پـردازی حسـن اجرای قوانین و دستورالعمل‌های ابـلاغ شـده را بـیش از پـیش کنترل نمایند.

# نقش ابزار فناوري اطلاعات در كنترل

- به طور مثال دقت‌نظر بسیاری از سازمان‌ها در نظارت بر حضور کارکنان و عدم امکان اشتباه در حضور و غیاب، باعث شده‌است که تجهیزات رایانه‌ای، معضلات مربوط به تفاوت نظر کارکنان و محاسبات حقوقی آنها را تسهیل نماید.
- لذا در صورتی که این نوع نگاه سیستماتیک در ارکان دیگر نظارت نیز مورد توجه قرار گیرد، مسلماً ضمن تسهیل امور مدیریتی، باعث بالارفتن راندمان اجرایی پروژه‌ها و در نهایت تأثیرپذیری روند توسعه در امور اقتصادی، اجتماعی، سیاسی، فرهنگی و... خواهد گردید.
- به همین دلیل است که نوع مدیریت دولت الکترونیک در بسیاری از کشورها از جمله ایران در دست بررسی و یا اجرا می‌باشد.

# نقش ابزار فناوري اطلاعات در كنترل

- این فناوری زمانی اثربخش خواهد بود که بتواند به نیازهای سازمان پاسخ دهد.
- بنابراین باید به صورت دوره‌ای ارزیابی شود تا با شناخت نارسایی‌های احتمالی آن در جهت بهبود سیستم اقدام شود.
- در واقع مدیران برای غلبه بر پیچیدگی ذاتی این فناوری باید دارای سیستم‌های کنترلی مؤثرتر و استقرار واحدهای فناوری اطلاعات و ارتباطات متناسب با نیازها در سازمان خود باشند.

# کنترل دسترسي

- یکی از اصلی ترین وظایف امنیت ، کنترل دسترسی به منابع است .
- کنترل دسترسی خیلی بیشتر از این است که تعیین کنیم که یک کاربر بتواند از یک فایل یا سرویس استفاده کند یا نه.
- کنترل دسترسی در حقیقت در مورد رابطه بین اشیاء یا **Object** ها و موضوع ها یا **Subject**ها صحبت می‌کند.
- یک موضوع یا **subject** یک موجودیت غیرفعال محسوب می‌شود، این موجودیت غیرفعال از طریق فرآیندی به نام دسترسی به دنبال بدست‌آوردن داده از قسمت‌های فعال یا همان اشیاء (**object**) هستند.
- یک موضوع می‌تواند شامل یک کاربر، یک برنامه، یک پایگاه‌داده، یک پروسس، یک فایل و ... باشد. یک شیء می‌تواند یک کاربر، فایل، کامپیوتر، پایگاه‌داده، پرینتر، دستگاه ذخیره‌سازی و از این قبیل باشد.

# کنترل دسترسي

- موضوع یا **subject** همیشه موجودیتی است که اطلاعات یا داده ها را درباره اشیاء یا **Object** ها بدست‌می‌آورد، همچنین این موجودیت اطلاعات یا داده‌های ذخیره شده در اشیاء را می‌تواند اصلاح کند.
- اشیاء همیشه موجودیت‌هایی هستند که اطلاعات یا داده‌ها را ارائه می‌دهند و یا میزبان اطلاعات هستند.
- نقش بین اشیاء و موضوع‌ها را می‌توان ارتباط بین نرم‌افزار و پایگاه‌داده و یا یک فایل و پروسس آن تصور کرد که برای انجام یک عملیا ت یا وظیفه در کنار هم جمع‌شده‌اند.

# کنترل دسترسي

- وجود کنترل‌های دسترسی برای حفظ محرمانگی، صحت یا تمامیت و دسترسی‌پذیری اشیاء (اطلاعات و داده‌ها) ضروری است.
- واژه کنترل دسترسی محدوده وسیعی از کنترل‌ها را در بر می‌گیرد که می‌تواند از مجبور کردن یک کاربر به استفاده از نام کاربری و رمز عبور معتبر برای ورود به سیستم باشد تا جلوگیری از دسترسی کاربران به منابع خارج از محدوده دسترسی اعمال شده برای آنان.
- کنترل‌های دسترسی از نظر نوع فعالیت و همچنین هدفی که برای آن طراحی شده‌اند به هفت گروه اصلی طبقه‌بندی می‌شود.
- همیشه در نظر داشته‌باشید که برخی از مکانیزم‌های امنیتی هستند که از چندین نوع از این گروه‌ها تشکیل شده‌اند و ترکیبی از این هفت گروه هستند:

# انواع کنترلهاي دسترسي

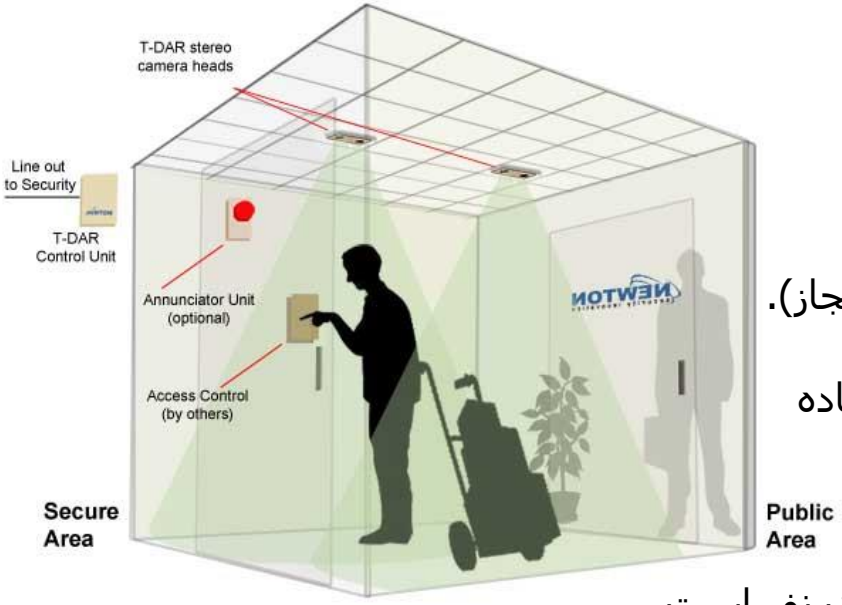
- کنترل های دسترسی پیشگیری کننده ( Preventative Access Control)
- کنترل های دسترسی منع کننده (Deterrent Access Control)
- کنترل های دسترسی شناسایی ( Detective Access Control)
- کنترل های دسترسی اصلاح کننده ( Corrective Access Control)
- کنترل های دسترسی ترمیمی یا بازیافتی ( Recovery Access Control)
- کنترل های دسترسی جبران کننده ( Compensation Access Control)
- کنترل های دسترسی دستوری ( Directive Access Control)

# کنترل های دسترسی پیشگیری کننده (Preventative Access Control)

- کنترل‌های دسترسی پیشگیری‌کننده از به وقوع پیوستن فعالیت‌های ناخواسته یا غیرمجاز جلوگیری می‌کنند. نمونه‌هاي زیر جزئی از کنترل های دسترسی پیشگیری کننده محسوب می‌شوند.

- ✓ فنس‌کشی‌ها
- ✓ قفل‌ها
- ✓ تجهیزات تشخیص هویت و شناسایی افراد
- ✓ **Mantrap**
- ✓ سیستم‌های روشنایی
- ✓ سیستم‌های هشداردهنده یا آلارم
- ✓ تقسیم وظایف
- ✓ تغییر چرخشی فعالیت ها ( job rotation)
- ✓ طبقه‌بندی اطلاعات
- ✓ تست نفوذسنجی
- ✓ رمزنگاری اطلاعات
- ✓ پایش و مانیتورینگ
- ✓ دوربین‌های مداربسته
- ✓ کارت‌های هوشمند
- ✓ سیستم‌های callback
- ✓ خط‌مشی‌های امنیتی
- ✓ برگزاری دوره‌های آموزشی امنیتی کارمندان
- ✓ نرم افزار های آنتی ویروس

# Mantrap

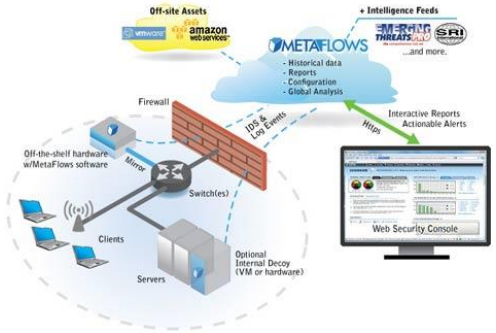



یکی از رایج‌ترین حفره‌ها و نقاط کور موجود در سیستم‌های کنترل دسترسی، امکان عبور افراد غیرمجاز از نقاط بازرسی از طریق متابعت یکی از کارکنان مجاز است.
(مانند باز نگهداشتن در پس از عبور و برای رد شدن فرد غیرمجاز).
یا ممکن است فرد غیرمجاز بی سروصدا و بدون جلب توجه این‌کار را انجام بدهد، راه‌حل سنتی جلوگیری از این‌کار، استفاده از فضای کوچکی به نام Mantrap است که در نقاط ورودی و خروجی به کار گرفته می‌شود. ساختار Mantrap بدین‌گونه است که در نقطه مورد نظر از دو در استفاده می‌شود که حجم فضای میان آن‌ها تنها به اندازه یک نفر است .
از این روش می‌توان در طراحی دستگاه‌های کنترل دسترسی و در نقاط ورودی و خروجی یا فقط در نقاط خروجی استفاده نمود. در حالتی که خروج فرد ناموفق باشد، سیستم امنیتی ضمن قفل کردن درها، اقدام به پخش آژیر اخطار می‌نماید و اعلام می‌کند که فرد مهاجم در تله Mantrap گرفتار شده است. روش دیگر جلوگیری از چنین مواردی، استفاده از کفپوش‌های مخصوصی است که با ثبت جای پای فرد، سیستم را از عبور تنها یک نفر در آن واحد مطمئن می‌سازد.
در فناوری جدیدی که برای حل این مشکل به کار گرفته شده است، با استفاده از یک دوربین حساس به حرکت (Motion Sensor) که در بالای اتاق نصب می‌شود، عبور افراد به طور خودکار تحت نظر گرفته می‌شود و چنانچه بیش از یک نفر در آن واحد در حال عبور باشند، سیستم امنیتی را فعال می‌سازد.

# کنترل های دسترسی منع کننده (Deterrent Access Control)

- کنترل‌های دسترسی منع‌کننده باعث دلسرد شدن از تخطی و دور زدن خط مشی‌های امنیتی می‌شوند. این کنترل‌ها زمانی کاربرد دارند که کنترل‌های دسترسی پیشگیری‌کننده نتوانسته‌اند به خوبی عمل کنند. یک کنترل دسترسی منع‌کننده هیچ فعالیتی را متوقف نمی‌کند و یا از وقوع آن جلوگیری نمی‌کند در عوض نتایج تخطی را تحت تأثیر قرار می‌دهد، برای مثال در صورتیکه تلاش یا هرگونه تخطی صورت بگیرد اینگونه کنترل ها وارد کار می‌شوند. نمونه‌هاي زیر نوعی از کنترل های دسترسی منع کننده محسوب می شوند.

- ✓ قفل‌ها
- ✓ فنس‌ها
- ✓ گارد حفاظتی
- ✓ دوربین‌های امنیتی
- ✓ تجهیزات اعلام هشدار
- ✓ تقسیم وظایف
- ✓ دستورالعمل‌های انجام کار
- ✓ دوره‌های آموزشی
- ✓ آگاه‌سازی امنیتی کارکنان
- ✓ رمزنگاری
- ✓ پایش و مانیتورینگ
- ✓ دیواره های آتش یا فایروال‌ها



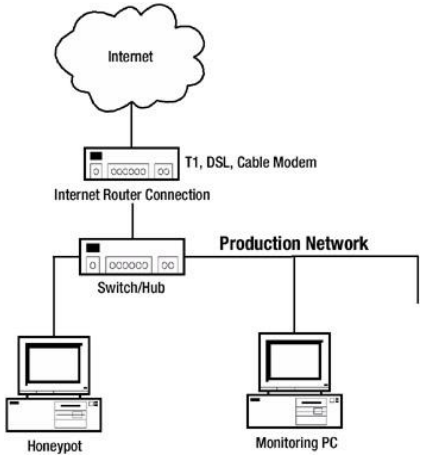
# کنترل های دسترسی
# شناسایی (Detective Access Control )

- کنترل‌های دسترسی شناسایی زمانی فعالیت می‌کنند که بخواهیم فعالیت‌های ناخواسته یا غیر مجاز را شناسایی کنیم. اینگونه کنترل‌ها همیشه در زمانی فعال می‌شوند که عمل ناخواسته یا غیر مجاز انجام شده‌است و کنترلی نیستند که بصورت بلادرنگ فعالیت کنند. موارد زیر نمونه‌هایی از کنترل های امنیتی شناسایی هستند.

- ✓ نگهبانان امنیتی
- ✓ سگ‌های نگهبان
- ✓ سیستم‌های تشخیص حرکت
- ✓ دوربین‌های مداربسته
- ✓ تغییرات شغلی مرحله ای ( job Rotation)
- ✓ فرستادن کارمندان به تعطیلات اجباری
- ✓ پایش و مانیتورینگ مداوم
- ✓ سیستم‌های تشخیص نفوذ
- ✓ هانی پات ها(Honeypot)
- ✓ گزارش‌های تخلف
- ✓ سرپرستی و نظارت درست بر عملکرد کارمندان و شناسایی بحران ها

# هانی‌پات (Honeypot)

- **هانی‌پات (Honeypot)** یک منبع سیستم اطلاعاتی با اطلاعات کاذب است که برای مقابله با هکرها و کشف و جمع‌آوری فعالیت‌های غیرمجاز در شبکه‌هاي رايانه‌اي بر روی شبکه قرار می‌گیرد.
- هانی‌پات‌ها کامپیوترهایی هستند که ابزاری برای مصالحه هستند، کامپیوترهایی که یا واقعی هستند و یا شبیه‌سازی شده‌اند.




- هانی پات یک منبع سیستم اطلاعاتی می‌باشد

که بر روی خود اطلاعات کاذب و غیر واقعی دارد و با استفاده از ارزش و اطلاعات کاذب خود سعی می‌کند اطلاعات و فعالیت‌های غیر مجاز و غیر قانونی بر روی شبکه را کشف و جمع‌آوری کند. به زبان ساده هانی‌پات یک سیستم یا سیستمهای کامپیوتری متصل به شبکه و یا اینترنت است که دارای اطلاعات کاذب بر روی خود می‌باشد. از عمد در شبکه قرار می‌گیرد تا به عنوان یک تله عمل کرده و مورد تهاجم یک هکر یا نفوذگر قرار بگیرد. با استفاده از این اطلاعات آنها را فریب داده و اطلاعاتی از نحوهٔ ورود آنها به شبکه و اهدافی که در شبکه دنبال می‌کنند، جمع‌آوری می‌کند.

# کنترل های دسترسی اصلاح کننده (Corrective Access Control)

- کنترل‌های دسترسی اصلاح‌کننده زمانی شروع به فعالیت می‌کنند که عمل ناخواسته یا دسترسی غیرمجاز ایجاد شده و سیستم دچار مشکل شده‌است و می‌بایست اصلاحات لازم جهت بازگردانی فعالیت به حالت معمول انجام گیرد. ذاتاً اینگونه کنترل‌های دسترسی ساده هستند و می‌توانند شامل پایان دادن به یک پروسس و یا دسترسی به فایل و یا راه‌اندازی مجدد یک سیستم باشند. کنترل‌های دسترسی اصلاح کننده معمولاً خیلی کم مي‌توانند بر روی دسترسی‌های غیرمجاز و سوء استفاده از دسترسی‌ها تأثیرگذار باشند و می‌توانند شامل سیستم های زیر باشند.
  - ✓ تشخیص نفوذ
  - ✓ راهکارهای آنتی ویروس
  - ✓ هشدار دهنده ها یا آلارم ها
  - ✓ طرح های تداوم کسب و کار و خط مشی های امنیت

# کنترل های دسترسی ترمیمی یا بازیافتی (Recovery Access Control )

- از کنترل‌های دسترسی ترمیمی یا بازیافتی زمانی استفاده می‌شود که بخواهیم پس از وقوع تخطی از خط مشی امنیت، منابع، فعالیت‌های عملیاتی و قابلیت‌ها را تعمیر یا بازیابی کنیم. کنترل‌های دسترسی ترمیمی نسبت به کنترل‌های دسترسی اصلاح‌کننده در زمان بروز تخطی از دسترسی‌ها، برای پاسخگویی قابلیت‌های پیشرفته‌تر و همچنین امکانات بیشتری دارند. برای مثال کنترل‌های دسترسی ترمیمی می‌توانند ضمن اینکه خرابی‌های بوجود آمده را ترمیم‌کنند، روند تخریبی آن را نیز متوقف‌کنند. نمونه‌هاي زير كنترل‌هاي ترميمي هستند.
  - ✓ نسخه های پشتیبان و بازگردانی ( Restore & Backup)
  - ✓ درایو های سیستم با قابلیت خطاپذیری یا redundancy
  - ✓ کلاسترینگ سرورها
  - ✓ نرم افزار آنتی ویروس و همچنین database shadowing یا mirroring

# کنترل های دسترسی جبران کننده (Compensation Access Control )

- کنترل‌های دسترسی جبران‌کننده یا جبرانی امکانات متنوعی را به سایر کنترل‌های دسترسی جهت کمک‌کردن به پشتیبانی و اجبار براي اعمال شدن خط‌مشی امنیت در اختیار می‌گذارند. برای مثال خط مشی امنیت، نظارت و سرپرستی کارکنان، مانیتورینگ یا پایش و دستورالعمل‌های انجام وظایف کاری از انواع کنترل‌های دسترسی جبرانی یا جبران‌کننده می‌باشند.
- از کنترل های دسترسی جبران‌کننده می‌توان به عنوان جایگزین به جای برخی دیگر از کنترل‌ها که دارای خطرات احتمالی هستند نیز استفاده کرد.
- برای مثال اگر می‌خواهید از محلی محافظت کنید که در آنجا مکان مسکونی وجود دارد بنابراین استفاده از سگ‌هاي نگهبان می‌تواند خطرناک باشد، در اینجا شما می‌توانید به جای سگ نگهبان از سیستم‌های تشخیص حرکت با قابلیت پخش صدای پارس سگ استفاده کنید که بسیار مؤثرتر و کم خطرتر از خود سگ است.

# کنترل های دسترسی دستوری
# (Directive Access Control )

- کنترل‌های دسترسی دستوری زمانی بکار می‌روند که بخواهیم با دستور و محبوس کردن و کنترل‌کردن فعالیت‌های یک موضوع آنرا مجبور به پذیرفتن خط مشی‌های امنیتی کنیم. از انواع کنترل‌های دسترسی دستوری می‌توان به گاردهای امنیتی، سگ‌هاي نگهبان، خطمشی امنیتی ، اخطاریه های ارسالی ، مانیتورینگ و پایش ، آموزش‌های امنیتی کارکنان و تقسیم وظایف کاری اشاره کرد.
- کنترل‌های دسترسی می‌توانند بر اساس روش پیاده‌سازی نیز طبقه‌بندی شوند.
  - ✓ **مدیریتی**
  - ✓ **منطقی یا فنی**
  - ✓ **فیزیکی**

# انواع کنترلهاي دسترسي براساس روش پياده سازي

- کنترل های دسترسی مدیریتی (Administrative Access Controls)
- کنترل‌های دسترسی منطقی یا فنی(Technical\Logical Access Controls)
- کنترل های دسترسی فیزیکی ( Physical Access Controls)

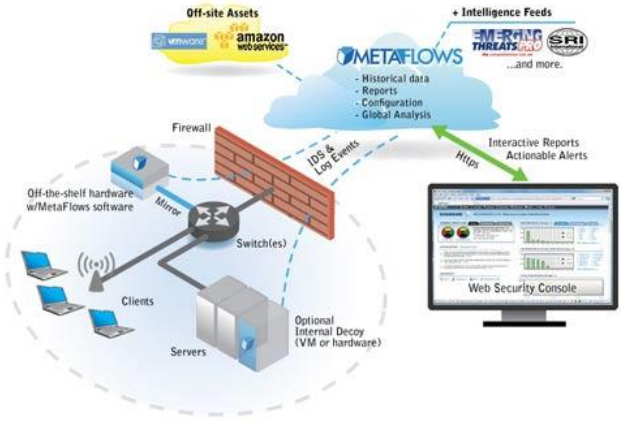
# کنترل های دسترسی مدیریتی
# (Administrative Access Controls )

- کنترل‌های دسترسی مدیریتی خط مشی‌ها و دستورالعمل‌هایی هستند که توسط خط مشی امنیتی سازمان برای اجبار به پیاده‌سازی سراسری کنترل‌های دسترسی تعریف شده‌اند. کنترل‌های دسترسی مدیریتی بیشتر بر روی دو موضوع کارکنان و فعالیت‌های تجاری (مردم و خط‌مشی‌ها) تمرکز می‌کنند. نمونه‌هاي زیر از انواع کنترل‌های دسترسی مدیریتی می‌باشند.

- ✓ خط مشی‌ها
- ✓ دستورالعمل‌ها
- ✓ بررسی کردن عدم سوءپیشینه
- ✓ طبقه‌بندی داده ها
- ✓ آموزش‌های امنیتی
- ✓ نظارت بر انجام کارها
- ✓ کنترل کردن کارکنان
- ✓ انجام تست های مختلف

# کنترل های دسترسی منطقی یا فنی (Technical\Logical Access Controls )

- کنترل‌های دسترسی منطقی و کنترل‌های دسترسی فنی مکانیزم‌های سخت‌افزاری و نرم‌افزاری هستند که بوسیله محافظت از منابع و سیستم‌ها دسترسی به آنها را کنترل و مدیریت می‌کنند. برای مثال:
  - ✓ رمزنگاری
  - ✓ کارت‌های هوشمند
  - ✓ رمزهای عبور
  - ✓ سیستم‌های تشخیص هویت biometric
  - ✓ لیست کنترل‌های دسترسی یا (ACL)
  - ✓ پروتکل‌ها
  - ✓ فایروال‌ها
  - ✓ مسیریاب‌ها و سیستم‌های تشخیص نفوذ




- برخی از انواع کنترل‌های دسترسی منطقی یا فنی هستند، در این موضوع کنترل دسترسی فنی و منطقی را می‌توان در کنار هم استفاده کرد.

# کنترل های دسترسی فیزیکی
# (Physical Access Controls )

- کنترل‌های دسترسی فیزیکی حصارها و موانع فیزیکی هستند که از دسترسی مستقیم و غیرمجاز به سیستم‌ها و منابع جلوگیری می‌کنند.

برای مثال:

- ✓ گاردهای امنیتی
- ✓ فنس‌ها
- ✓ سیستم‌های تشخیص حرکت
- ✓ درب‌های قفل‌شده
- ✓ پنجره‌های مهر و موم شده
- ✓ سیستم‌های روشنایی
- ✓ سیستم‌های محافظت از کابل‌کشی
- ✓ قفل‌های لپ‌تاپ
- ✓ سگ‌های نگهبان
- ✓ دوربین‌های امنیتی و سیستم های هشدار دهنده یا آلارم

از انواع کنترل های دسترسی فیزیکی هستند.

# کنترل های دسترسی

- شما هیچوقت جایی را پیدا نخواهید کرد که صرفاً از یک نوع مکانیزم کنترل دسترسی استفاده کرده‌باشد. در حقیقت تنها راهی که می‌توان به وسیله آن محیطی ایمن داشت، محلی است که از چندین کنترل دسترسی بصورت ترکیبی استفاده کرده‌است.

# نمونه هايي از انواع كنترلها توسط ابزار فناوري اطلاعات

- كنترل هوشمند تردد و ترافيك بزرگراه‌ها ( CCTV )
- ردیابي وسايل حمل و نقل عمومي
- سيستم عوارض خودرويي ساليانه و عوارض جاده‌اي
- جلوگيري ازسرقت اتومبيل
- سيستم كروز در اتومبيل
- سيستم اعلام خطر در اتومبيل (دزدگير)
- استفاده از GPS تلفن همراه در كنترل ترافيك
- سيستم اطفاء حريق
- سيستم تهويه هوشمند
- سيستم پارك هوشمند حاشيه
- سيستم هوشمند مديريت و كنترل پاركينگ
- استفاده از تگ‌ها RFID در انواع كنترل‌ها

# نتيجه گيري

- کنترل سبب امنيت اطلاعات مي‌گردد.
- سرعت تغييرات در فناوری اطلاعات و ارتباطات بسيار زياد است، آيا ما می‌توانيم با اين تغييرات همسان باشيم؟
- برای دست‌يافتن به سطح مطلوب امنيت فناوری اطلاعات و ارتباطات بايد تغيير نگرش اساسی در مديران سازمانی و مديران فناوری اطلاعات اتفاق بيايد.
- بر اين اساس کنترل و امنيت فناوری اطلاعات و ارتباطات بايد دغدغه همگان باشد.

# دو آیه  قرآن در مورد کنترل

«آیا او نمی‌داند که خدا همه اعمالش را می بیند» ( سوره علق، آیه ١٤ )

«آیا انسان گمان می کند که کسی او را نمی‌بیند» ( سوره بلد، آیه٧ )

# فهرست منابع


شبکه فناوری اطلاعات ایران
استونر، جیمز فریمن . ادوارد، مدیریت رفتار سازماني (جلد سوم : رهبري و کنترل).
سـيد محمـد اعرابـي و علـي پارسـائيان، تهـران : مؤسسـه مطالعـات و پژوهشـهاي بازرگاني، 1375
دیوید، فرد، آر؛ مدیریت استراتژیک، ترجمه دکتراعرابی، دفتر پژوهشهای فرهنگی، تهران، 1380
رضائيان. علي، اصول مدیریت، سمت، 1369
http://security.itpro.ir/articles
https://cert.um.ac.ir/index.php?=Article/index

با تشکر از همراهي استاد گرامي

و شما همکلاسي هاي محترم

# پایان