کاربرد فناوری اطلاعات و ارتباطات

مدرس: مسعود معاونی

منبع تدریس: کتاب کاربرد فناوری اطلاعات و ارتباطات آقای جعفرنژاد قمی
انتشارات دانشگاه جامع علمی کاربردی به همراه نکات تکمیلی در فایل پاورپوینت مدرس

ترم اول سال ۴۰۳- ۱۴۰۴

فصل نهم: امنیت اطلاعات

- با توجه به ویژگی‌های امروزی که عصر اطلاعات نامیده می‌شود، مهمترین سرمایه برای هر فرد یا سازمان، اطلاعات است. از همین رو حفظ امنیت اطلاعات و محرمانگی داده‌ها اهمیت زیادی دارد. امنیت اطلاعات به حفاظت از اطلاعات و کاهش خطر افشای اطلاعات توسط عوامل غیرمجاز اشاره دارد.
- آرمانی‌ترین حالت در امنیت اطلاعات زمانی است که تمهیدات امنیتی در شبکه، وب‌سایت‌ها یا نرم‌افزارهای کامپیوتری برای کاربران مجاز و خودی اصلت به چشم نیاید و اصطلاحا سیستم شفاف باشد، این در حالی است که در همان وضعیت کاربران غیرمجاز با یکحصار تاریک و غیر قابل نفوذ مواجه شوند.
- امنیت اطلاعات همیشه یک شمشیر دو لبه است. یعنی عدم توجه به حفاظت کامل از اطلاعات، مشکلات سایبری و هک را به‌وجود می‌آورد و توجه بیش از حد به امنیت سایبری باعث آزار و کاهش سرعت دسترسی کاربران مجاز به اطلاعات می‌شود.

آشنایی با اصول امنیت اطلاعات

- امنیت در هر سیستم کامپیوتری از سه اصل مهم تشکیل می‌شود:
  - محرمانگی یا Confidentiality که معنای آن این است که اطلاعات فقط در اختیار افرادی قرار گیرد که مجاز به دسترسی به آن هستند. خروج اطلاعات محرمانه از سیستم یک شرکت یا سیستم فردی، عاملی برای حملات و تهدبدات امنیتی بعدی می‌باشد.
  - جامعیت یا Integrity مفهومی است که به علوم کگامپیوتری بر می‌گرد و شامل این نکته کلیدی می‌شود که اگر تغییری در اطلاعات یا فرایندهای مشخص و مجاز انجام شود، باید در تمامی سیستم‌های داخل و بیرونی انجام شود. همزمانی عملیات در سرورها و پایگاه‌های داده بخش مهمی از جامعیت اطلاعات را تشکیل می‌دهد.
  - دسترس‌پذیری Avalibility در امنیت اطلاعات به این موضوع اشاره می‌کند که سامانه‌های کامپیوتری باید همیشه برای افراد مجاز در دسترس باشند. اگر به هر دلیلی سامانه‌ای از دسترس خارج شود نوعی تهدید امنیتی محسوب می‌شود.


امنیت اطلاعات

مفهوم احراز هویت

- در کنار سه اصل کلیدی که درباره امنیت اطلاعات گفته شد، موضوعات زیر نیز حائز اهمیت هستند:
  - احراز هویت یا Authentication از موضوعاتی است که باید مورد توجه قرار گیرد. برای احراز هویت روش‌های متنوعی در سیستم‌های سایبری وجود دارد.
  - میزان دسترسی کاربر یا Authorization از موضوعاتی است که امکان دسترسی مجاز هر کاربری را به اطلاعات را نشان می‌دهد.
  - قابلیت حسابرسی و ثبت لاگ یا همان Accountability که موجب می‌شود تا دسترسی به منابع و استفاده از اطلاعات قابل پیگیری باشند.

انواع روش‌های احراز هویت

- برای احراز هویت از چند فاکتور کلیدی استفاده می‌شود:
  - **فاکتور اول: چیزی که شما می دانید : مثل رمز عبور**
  - **فاکتور دوم: چیزی که شما دارید : مثل کارت بانکی**
  - **فاکتور سوم : چیزی که شما هستید: مثل بیومتریک**
  - **فاکتور چهارم: کاری که شما می کنید: مثل سرعت تایپ یا نوع راه رفتن و...**
  - **فاکتور پنجم: احراز هویت چند فاکتوری**

پیاده‌سازی امنیت اطلاعات

- برای پیاده‌سازی امنیت اطلاعات ۶ گام اساسی زیر باید اجرا شود:
  ۱. توسعه، تصویب و ترویج خط مشی امنیت اطلاعات فراگیر
  ۲. آگاهی و پاسخگویی تمامی کارکنان درباره امنیت اطلاعات سازمان
  ۳. ایجاد امور امنیت اطلاعات در هر بخش سازمان
  ۴. گزارش‌گیری مستمر و منظم از فرایندهای امنیت اطلاعات در سازمان و ارائه به مدیران ارشد؛
  ۵. پیاده کردن کنترل‌های فعال و گسترده
  ۶. بروزرسانی مستمر نرم‌افزارها و کنترل فرایندها برای جلوگیری از نفوذ به سیستم‌ها

ابعاد مرتبط با امنیت اطلاعات

- بسیاری از تهدیدات و مشکلات امنیتی در سیستم‌های اطلاعاتی از سه بُعد زیر ایجاد می‌شوند:
  - امنیت فیزیکی: حفاظت از کامپیوترها، سرورها و پایگاه‌های اطلاعاتی دربرابر سرقت، آتش‌سوزی عمدی یا دسترسی غیرمجازافراد به آنها است. بسیاری از تهدیدات امنیتی با نصب یک فلش آلوده به بدافزار ایجاد می‌شوند. آشنایی کارکنان و مدیران فناوری با اینگونه از مشکلات امنیتی در هر سازمانی ضروری است.
  - امنیت عملیاتی: مدیریت اطلاعات از بخش‌های مهم در امنیت سایبری است. کنترل دسترسی، شناسایی و تعیین توپولوژی شبکه (مکان‌شناسی افراد) از بخش‌های مهم در امنیت عملیاتی است. تهیه نسخه پشتیبان، اتصال به شبکه‌های دیگر، بازگردانی اطلاعات، بروزرسانی نرم‌افزارها، تغییر رمزهای عبور به‌صورت دوره‌ای و... در بخش امنیت عملیاتی قرار می‌گیرند.
  - مدیریت و خط مشی‌ها: مدیریت سازمانی نقش مهمی در بهبود امنیت اطلاعات دارند. تصمیم‌هایی که باید در سطح مدیریت و سیاست‌های کلان گرفته شوند باعث افزایش امنیت سایبری در هر شرکتی می‌شوند.

حفاظت از اطلاعات

- برای حفظ اطلاعات در هر سازمانی باید به سه گام کلیدی زیر توجه کرد:
  - پیشگیری و حفاظت
  - تشخیص
  - واکنش

آشنایی با انواع فناوری‌های امنیت اطلاعات

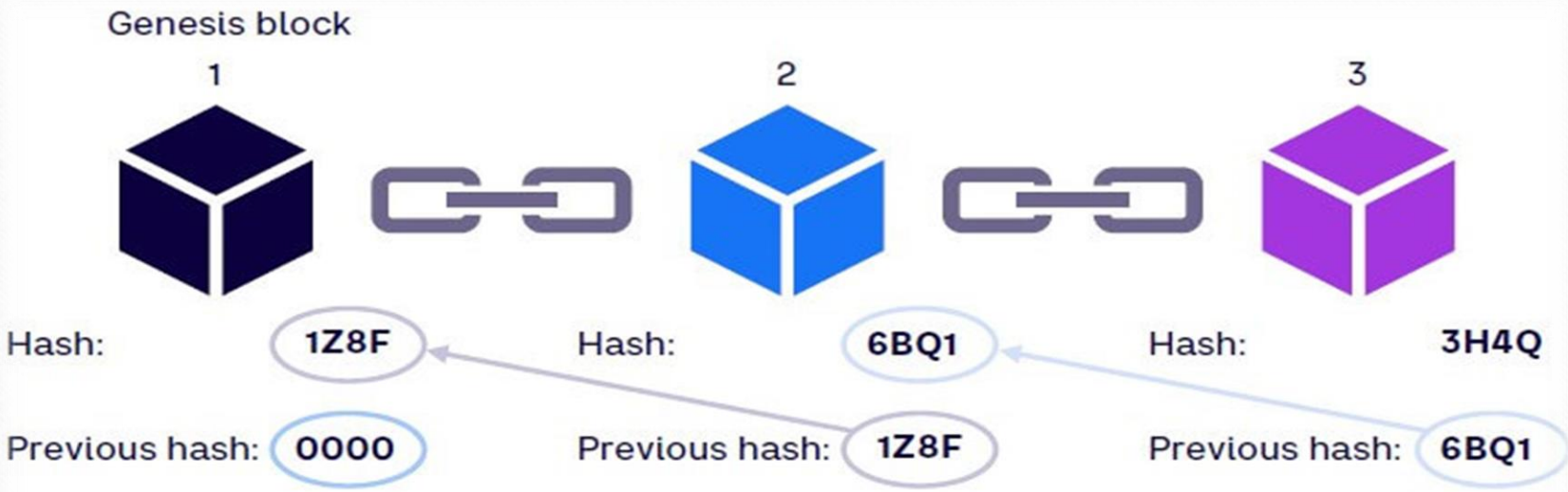
- برای حفظ امنیت اطلاعات در هر سازمانی، برحسب زمان و سطح سازمانی از فناوری‌های مختلفی استفاده می‌شود. هر فناوری هزینه متفاوتی داشته و البته نتایج خاص خود را برای امنیت سایبری به همراه می‌آورد:

۱- رمزنگاری Cryptography

- در این روش اطلاعات آشکار به شیوه‌های مختلفی رمز شده تا توسط دیگران قبل خواندن نباشند. در رمزنگاری از یک کلید رمز خصوصی برای رمزگذاری و از یک کلید رمز عمومی برای رمزگشایی استفاده می‌شود. اگر چه در الگوریتم‌های رمزنگاری امنیت اطلاعات بالایی وجود دارد اما افشای کلیدهای رمز امنیت این سیستم‌ها را به خطر می‌اندازد.
- برخی از روش‌های رمزنگاری معرف عبارتند از Des، MD5، SHA1، SHA2 و...

۲- فناوری بلاکچین

- اگر چه روش‌های رمزنگاری امنیت خوبی دارند اما در مواردی شاهد حملات امنیتی به پروتکل‌های رمزنگاری هستیم. امروزه بلاکچین امنیت بالاتری نسبت به روش‌های رمزنگاری سنتی دارد:



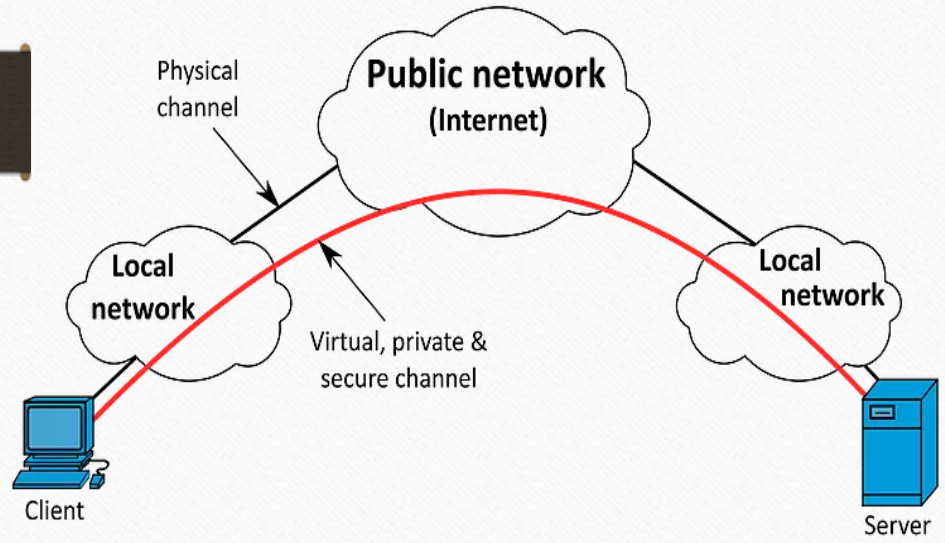
۳- امضای دیجیتال

- امضای دیجیتال یک روش رمزنگاری است که برای تأیید هویت فرستنده و اطمینان از صحت محتوا در اسناد الکترونیکی استفاده می‌شود. این امضاها با استفاده از الگوریتم‌های پیچیده‌ای مانند RSAو DSAتولید می‌شوند و شامل دو کلید اصلی هستند: کلید عمومی و کلید خصوصی. کلید خصوصی برای ایجاد امضا استفاده می‌شود و باید به شدت محافظت شود، در حالی که کلید عمومی برای تأیید صحت امضا به کار می‌رود.

۴- قراردادهای هوشمند

- **قرارداد هوشمند** یا همان **اسمارت کانترکت** (**Smart Contract)**برنامه یا کدی است که روی بلاک چین ذخیره می‌شود و در صورت رخدادن شرایط خاص، **بدون واسطه** و بدون نیاز به تأیید کسی اجرا خواهد شد. مفهوم این قراردادها اولین بار توسط ن**یک زابو** (**Nick Szabo)**در سال **۱۹۹۴** ارائه شد.
- قراردادهای هوشمند به نوعی نوشته می‌شوند که پس از اجرا و تحقق همه طرفین از صحت اجرای آن **مطمئن** باشند و پای **واسطه** در قرارداد **حذف** شود.
- جذابیت اصلی قرارداد هوشمند آنجاست که وقتی اجرا می‌شود، حتی خود توسعه‌دهنده هم نمی‌تواند مانع اجرای آن شود، مگر آنکه پیش از اجرا فکر آن را کرده باشد. برای همین است که پس از اجرا همه طرفین از درست اجراشدن آن مطمئن هستند.

۵. شبکه مجازی خصوصی VPN



- برای اتصال به یک شبکه خصوصی از راه دور و از طریق یک شبکه عمومی لازم است یک شبکه خصوصی مجازی ایجاد کنید. این اتصال از طریق یک تونل رمزنگاری شده بین کلاینت VPNو شبکه خصوصی شما صورت میپذیرد. شما با وارد کردن یک نام کاربری و کلمه عبور و یا وارد کردن یک Certificateدر نرم افزار کلاینت VPNمی توانید یک تونل امن به شبکه خصوصی مورد نظرتان باز کنید.

۶- آنتی ویروس‌ها و فایروال‌ها

- نرم‌افزارهای فایروال یا همان دیواره آتش وظیفه دارند که جلوی ورودهای غیرمجاز را بگیرند. **فایروال** یا دیواره آتش (Firewall)به نرم‌افزار یا سخت‌افزارهایی گفته می‌شود که از دسترسی به کامپیوترها جلوگیری کرده و ترافیک رد و بدل شده در شبکه را کنترل می‌کند. فایروال در حقیقت یک ابزار امنیتی است که می‌تواند یک برنامه‌ی نرم‌افزاری یا یک دستگاه اختصاصی شبکه باشد.
- نرم‌افزار آنتی ویروس یا در تعریف دقیق‌تر و به‌روزتر آنتی‌مالور (ضد بدافزار) ابزاری است که بر اپلیکیشن‌های موجود در کامپیوتر شخصی یا گوشی هوشمند، نظارت می‌کند. نرم‌افزار آنتی ویروس یک ابزار امنیت داده است که در یک سیستم کامپیوتری با هدف محافظت دربرابر ویروس‌ها، جاسوس‌افزارها، بدافزارها، روت‌کیت‌ها، تروجان‌ها، حملات فیشینگ، حملات اسپم و سایر تهدیدات سایبری آنلاین نصب می‌شود.
- ویروس هر برنامه ناخواسته‌ای است که بدون اطلاع کاربر وارد سیستم می‌شود، می‌تواند خود را تکثیر و گسترش دهد، اقدامات ناخواسته و مخربی را انجام دهد که در نهایت بر عملکرد سیستم و داده‌ها یا فایل‌های کاربر تأثیر می‌گذارد. ویروس کامپیوتری را می‌توان به‌عنوان یک بیماری کامپیوتری در نظر گرفت، درست مانند ویروس‌های انسانی که باعث بیماری در انسان می‌شود.

۷- گذرواژه‌ها

- رمز عبور یا همان Password یا گذرواژه مجموعه‌ای از حروف، اعداد و کاراکترها است که برای ورود به یک سیستم خاص مورد استفاده قرار می‌گیرد. انتخاب گذرواژه مناسب، بروزرسانی و حفظ امنیت آن بر روی ایمنی سیستم‌های سایبری تاثیر می‌گذارد.

۸- زیست سنجی یا بیومتریک

- احراز هویت بیومتریک یک فرآیند امنیتی است که مشخصات فرد را با مجموعه ای از داده های بیومتریک ذخیره شده مقایسه کرده و در صورت تایید، اجازه دسترسی به سامانه ها، برنامه ها و موارد دیگر را می دهد. با افزایش جرایم اینترنتی، کلاهبرداری و سرقت هویت، بیشتر از هر زمان برای کسب و کارها اهمیت دارد که به کارمندان و مشتریان خود برای احراز هویت کمک کنند. احراز هویت بیومتریک یکی از معتبرترین روش ها برای حل این مسئله است.

۹- واقعه نگاری یا Logging

- ثبت اعمال یا تراکنش‌های انجام شده توسط کاربر یا یک برنامه، تولید سابقه و ثبت نظام‌مند رویدادهای مشخص را واقعه‌نگاری یا لاگ فایل می‌نامیم.واقعه نگاری کمک زیادی به شناسایی عوامل امنیتی در یک شبکه می‌کند.

۱۰- نهان نگاری

- Steganographyیا نهان نگاری روش مخفی کردن داده های مهم در یک فایل یا پیام معمولی، به منظور جلوگیری از شناسایی توسط دیگران است؛ سپس این اطلاعات مخفی در مقصد به حالت اولیه استخراج می شوند. استفاده از استگانوگرافی می تواند با رمزگذاری به عنوان یک گام اضافی برای مخفی کردن یا محافظت از داده ها، ترکیب شود. کلمه steganographyاز کلمات یونانی steganosبه معنی پنهان یا پوشیده شده و ریشه یونانی graphبه معنی نوشتن گرفته شده است.

۱۱- جلوگیری از مهندسی اجتماعی

- حملات مهندسی اجتماعی اشکال مختلفی دارد و می توانند در هر جایی که با تعاملات انسانی دخیل است انجام شود. در ادامه چند شکل متداول از حملات مهندسی اجتماعی دیجیتال آورده شده است:
  - **طعمه گذاری مانند فیشینگ**
  - **ترس افزار مانند پیامک‌های تهدیدآمیز**
  - **نرم افزار تبلیغاتی**
  - **بهانه سازی مانند تهدید به افشای اطلاعات محرمانه**

۱۲- جلوگیری از حملات منع سرویس یا DDoS

- یک حمله منع سرویس توزیع شده، DDoS، یک حمله سایبری است که در آن یک حجم وسیع از ترافیک به سمت کامپیوترها ، سرورها، یا شبکه ای از آنها ارسال می شود تا از دسترسی کاربران عادی به آنها جلوگیری به عمل آید. می توانید این پروسه را شبیه به یک ترافیک جاده ای اما در اینترنت تشبیه کنید. حملات Ddos به‌طور معمول توسط بات‌نت‌ها ایجاد می‌شوند.

راهکارهایی برای حفاظت از اطلاعات شخصی

- فشرده‌سازی و رمزگذاری رو فایل‌ها با استفاده از نرم‌افزار winrar
- تهیه نسخه پشتیبان از اطلاعات مهم
- استفاده از رمز عبور مناسب و پیچیده برای ورود به سیستم‌های کامپیوتری
- تعویض دوره‌ای رمزهای عبور
- عدم افشا اطلاعات شخصی در فضاهای عمومی مانند شبکه‌های اجتماعی
- عدم بازگشایی ایمیل‌های ناشناخته
- استفاده از احرازهویت دو مرحله‌ای
- غیرفعال کردن موقعیت مکانی برای حفاظت از حریم خصوصی

پایان