Identificación, Autenticación, Autorización e Auditoría

Nos sistemas operativos modernos, a seguridade da información é un aspecto crítico que require unha xestión efectiva da identificación, autenticación, autorización e auditoría (IAAA). Estes catro elementos constitúen os fundamentos sobre os que se constrúe a seguridade informática, e a súa implementación adecuada é crucial para protexer os datos e recursos do sistema.

Identificación

A identificación é o proceso de recoñecer e asociar unha entidade (como un usuario, un dispositivo ou unha aplicación) cunha identidade única no sistema. Esta identidade pode ser representada por un nome de usuario, un número de identificación ou calquera outro identificador único. Nos sistemas operativos, a identificación é o primeiro paso para acceder aos recursos do sistema.

Windows: En sistemas Windows, a identificación é xestionada a través de contas de usuario locais ou contas de usuario de dominio, dependendo da configuración da rede. *O Directorio Activo (Active Directory)* é a ferramenta principal para xestionar identidades e acceso en entornos empresariais.

Linux: En sistemas Linux, os usuarios son identificados a través de nomes de usuario e IDs de usuario (UIDs). Os sistemas de autenticación como Pluggable Authentication Modules (PAM) e Lightweight Directory Access Protocol (LDAP) son comúns para xestionar identidades en sistemas Linux.

A xestión de identidades é unha parte fundamental da seguridade da información en entornos empresariais e en liña. Consiste na xestión eficiente das identidades dos usuarios, o acceso aos recursos e os datos asociados, garantindo a seguridade e a integridade das operacións.

Sistemas de xestión de identidades comúns son:

- **Os servizos de Directorio:** Utilizan normalmente unha base de datos de directorio (LDAP) e un mecanismo de autenticación (Kerberos) para xestionar as identidades da rede e xestionar a súa autenticación e autorización. A implantación de sistema de directorio máis coñecida é o ***Directorio Activo de Microsoft***, aínda que existen outras implantacións de outros fabricantes. En Linux, **samba4** proporciona unha implementación de un servizo de directorio cun grao de compatibilidade moi alto co Directorio Activo de Microsoft.
- **Oauth/OpenID**: OpenID é un sistema de autenticación único que permite aos usuarios autenticarse en múltiples sitios web ou aplicacións utilizando unha única identidade. O obxectivo é simplificar o proceso de autenticación para os usuarios e reducir a necesidade de crear e xestionar múltiples contas e contrasinais. O obxectivo principal de OAuth é permitir que os usuarios outorguen acceso a aplicacións ou servizos a certos recursos sen ter que compartir as súas credenciais de inicio de sesión. En lugar diso, OAuth permite que un usuario autorice unha aplicación a acceder aos seus datos en servizos en liña en nome deles. Mentres que OAuth trata da autorización para acceder a recursos, OpenID trata da autenticación do usuario. Unha vez que un usuario se autentica con OpenID nunha aplicación, a aplicación pode utilizar OAuth para acceder a recursos en nome do usuario sen ter que solicitar credenciais adicionais.
- **Radius/Tacacs:** ***RADIUS (Remote Authentication Dial-In User Service)*** e ***TACACS (Terminal Access Controller Access-Control System)*** son dous protocolos de autenticación e autorización utilizados en redes de computadoras. RADIUS é un protocolo de

autenticación e autorización amplamente utilizado en redes para permitir o acceso seguro a recursos de rede, como servidores, routers e switches a través dun servidor centralizado que xestiona a autorización e a autenticación. Unha implementación libre e común é freeRadius. TACACS é un protocolo semellante a RADIUS que se utiliza para controlar o acceso a recursos de rede. A principal diferencia entre TACACS e RADIUS é que TACACS separa a autenticación da autorización, proporcionando un maior control sobre o acceso aos recursos.

Autenticación

A autenticación é o proceso de verificar a identidade dunha entidade que intenta acceder a un sistema ou recurso. Este proceso require a presentación dunha credencial, como un contrasinal, unha chave de acceso ou unha biometría, que poida ser verificada polo sistema.

Factores de Autenticación

Un factor de autenticación é unha categoría ou tipo de información que se utiliza para verificar a identidade dun usuario antes de conceder o acceso a un sistema ou recurso. Na autenticación tradicional, normalmente só se require un factor, como un contrasinal. Con todo, na autenticación multifactor (AMF), requirense múltiples factores para aumentar a seguridade.

Os factores de autenticación poden clasificarse xeralmente en tres categorías principais:

- Algo que o usuario sabe: Este factor implica información que só o usuario debe coñecer. O exemplo máis común é un contrasinal ou un PIN. Ao requerir un contrasinal, o sistema está a verificar se o usuario ten coñecemento dunha secuencia específica de caracteres que se asociou previamente coa súa identidade.
- Algo que o usuario posúe: Este factor require que o usuario teña acceso físico a un dispositivo ou obxecto específico. Exemplos disto poden incluír un teléfono móbil, unha tarxeta de acceso físico ou unha chave de seguridade USB. Ao utilizar este factor, o sistema está a comprobar se o usuario ten en posesión algo que se asociou previamente coa súa identidade.
- Algo que o usuario é: Este factor implica unha característica biométrica única ou comportamento físico do usuario. Pode incluír características como a súa voz, a súa impresión dixital, o seu recoñecemento facial ou outras características biolóxicas únicas. Ao utilizar este factor, o sistema está a verificar se o usuario é fisicamente quen di ser.

A combinación de varios factores de autenticación, como un contrasinal (algo que o usuario sabe) e un código enviado a un dispositivo móbil (algo que o usuario posúe), é o que define a **autenticación multifactor**. Esta técnica aumenta considerablemente a seguridade ao requerir que un atacante teña acceso non só a un, senón a varios factores, antes de poder acceder ao sistema ou recurso protexido.

Factores de Autenticación Típicos

Algo que se sabe:

- Contrasinais: Os contrasinais son a forma máis común de factor de coñecemento. Consisten nunha secuencia de caracteres, como letras, números e símbolos, que o usuario debe introducir para demostrar que coñece a credencial correcta asociada á súa conta. Os

contrasinais poden variar en longitude e complexidade e deben ser mantidos en segredo polo usuario.

- Preguntas de seguridade: Estas son preguntas que requiren que o usuario responda con información persoal previamente establecida durante o proceso de rexistro. Pódense facer preguntas sobre datos persoais, como o nome da nai, a cidade natal ou a marca do primeiro coche. A resposta correcta á pregunta de seguridade confirma que o usuario posúe información coñecida só por eles.
- Frases de pase: Similar aos contrasinais, as frases de pase son secuencias de palabras ou frases que o usuario debe recordar e introducir para autenticarse. A diferenza dos contrasinais, as frases de pase son xeralmente máis longas e poden ser máis fáciles de recordar para os usuarios.
- PINs: Un PIN (número de identificación persoal) é unha secuencia de números que o usuario debe introducir para autenticarse. Os PINs son comúnmente utilizados en tarxetas de débito ou crédito, así como en sistemas informáticos e dispositivos electrónicos.
- Patrón de desbloqueo: Este método de autenticación é común en dispositivos móbiles e táctiles, onde o usuario debe debuxar un patrón específico sobre unha grade de puntos para desbloquear o dispositivo. O patrón de desbloqueo require que o usuario coñeza o patrón correcto para acceder ao dispositivo.

Algo que se ten:

- Tarxetas de acceso físico: Son tarxetas plásticas ou electrónicas que conteñen un chip ou banda magnética que pode ser lido por dispositivos de acceso. Estas tarxetas son comúns en sistemas de seguridade física, como os que controlan o acceso a edificios ou oficinas.
- Teléfonos móbil: Os teléfonos móbil son cada vez máis utilizados como factores de autenticación. Pódense enviar códigos de verificación por mensaxes de texto ou notificacións de aplicación para verificar a identidade do usuario. Ademais, as aplicacións de autenticación móbil, como Google Authenticator ou Microsoft Authenticator, xeran códigos temporais que o usuario debe introducir para acceder ao sistema.
- Chaves de seguridade USB: Estas son pequenas chaves USB que conteñen información de identificación e poden ser conectadas ao ordenador do usuario para completar o proceso de autenticación. As chaves de seguridade USB suelen usar estándares como FIDO U2F ou FIDO2 para proporcionar unha autenticación segura.
- Tarxetas inteligentes: Estas son tarxetas plásticas ou electrónicas que conteñen un microprocesador e poden ser utilizadas para autenticación en sistemas informáticos. Poden incluír certificados dixitais e chaves criptográficas para unha autenticación segura.
- Tokens de seguridade (Tokens RSA/OTP – One Time Password): Son dispositivos hardware pequenos que xeran códigos temporais ou únicos que o usuario debe introducir durante o proceso de autenticación. Estes códigos normalmente cambian cada poucos segundos e son utilizados xunto cun contrasinal para verificar a identidade do usuario.

Algo que se e:

- Biometría facial: A biometría facial implica a captura e análise de características faciais únicas dun individuo, como a forma da cara, a posición dos ollos e a estrutura do nariz. Os sistemas de autenticación facial utilizan algoritmos avanzados de recoñecemento de imaxes para verificar a identidade dun usuario comparando a súa cara coa información almacenada previamente.
- Biometría da voz: A biometría da voz implica a análise das características físicas e acústicas da voz dun individuo, como o tono, a entoación e a frecuencia das ondas sonoras. Os sistemas de autenticación da voz utilizan estas características para verificar a identidade dun usuario cando fala a un dispositivo habilitado para a autenticación da voz.
- Recoñecemento da íris: O recoñecemento da íris implica a captura e análise dos patróns únicos presentes na íris dun individuo, como a disposición dos vasos sanguíneos e os padróns de pigmentación. Os sistemas de autenticación da íris utilizan cámaras especializadas para capturar imaxes da íris e comparalas coa información almacenada previamente para verificar a identidade dun usuario.
- Recoñecemento da impresión dixital: O recoñecemento da impresión dixital implica a captura e análise dos patróns únicos presentes nas impresións dixitais dun individuo, como as cristas e os vales presentes nas polpas dos dedos. Os sistemas de autenticación da impresión dixital utilizan escáneres dixitais para capturar a impresión dixital dun usuario e comparala coa información almacenada previamente para verificar a súa identidade.
- Recoñecemento de retina: O recoñecemento da retina implica a captura e análise dos patróns únicos presentes na retina dun individuo, como os vasos sanguíneos e as estruturas nerviosas. Os sistemas de autenticación da retina utilizan escáneres de retina para capturar imaxes da retina e comparalas coa información almacenada previamente para verificar a identidade dun usuario.

Software e sistemas comúns para autenticación:

Windows: En sistemas Windows, a autenticación é xestionada polo servizo de autenticación de Windows (Windows Authentication Service), que verifica as credenciais de usuario introducidas ao acceder ao sistema.

Linux: Nos sistemas Linux, a autenticación pode ser xestionada por diferentes métodos, incluíndo contrasinais, chaves SSH, certificados e autenticación biométrica. As ferramentas como **PAM** e **Kerberos** son amplamente utilizadas para xestionar a autenticación en sistemas Linux.

Autorización

A autorización é o proceso de determinar os permisos e os recursos aos que unha entidade autenticada ten acceso no sistema. Esta etapa verifica os dereitos de acceso dun usuario ou unha aplicación e limita as súas accións segundo as políticas de seguridade definidas.

Software e sistemas comúns para autorización:

Windows: En sistemas Windows, a autorización é xestionada polas políticas de seguridade e os permisos de acceso configurados para os recursos do sistema. O Control de Acceso Discrecional

(DAC) e o Control de Acceso Obrigatorio (MAC) son mecanismos comúns para controlar a autorización en sistemas Windows.

Linux: En sistemas Linux, a autorización é xestionada polos permisos de arquivo e directorio, así como polas políticas de seguridade implementadas polo sistema. Sistemas como SELinux e AppArmor proporcionan capacidades avanzadas de autorización en sistemas Linux.

Control de Acceso Discrecional (DAC)

O control de acceso discrecional é un modelo onde os propietarios dos recursos teñen o poder para determinar quen pode acceder a eles e en qué medida. En sistemas Windows, isto reflíctese nas permisos de arquivo e nas políticas de seguridade. Por exemplo, un usuario pode especificar quen ten permiso para ler, escribir ou executar un arquivo.

En Linux, o sistema de permisos é semellante, con comandos como chmod e chown que permiten aos usuarios modificar os permisos de arquivo e directorio. O propietario do arquivo ou directorio pode outorgar ou rexeitar acceso a outros usuarios ou grupos, segundo as súas necesidades.

Control de Acceso Obrigatorio (MAC)

Ao contrario do DAC, no control de acceso obrigatorio, o sistema operativo é o que establece as políticas de seguridade e impónas de maneira rigorosa. Isto asegura que a información só se comparta de acordo coas normas definidas polo administrador do sistema, independentemente das preferencias dos usuarios individuais.

En Windows, o control de acceso obrigatorio é implementado a través de políticas de seguridade avanzadas e perfiles de seguridade, que permiten aos administradores controlar o acceso a nivel de sistema.

En Linux, os sistemas MAC máis comúns son SELinux (Security Enhanced Linux) e AppArmor. Estes sistemas impoñen políticas de seguridade a nivel do núcleo, asegurando que os accesos a recursos do sistema sexan estritamente controlados.

Auditoría

A auditoría é o proceso de rexistrar e analizar as accións realizadas por usuarios e aplicativos no sistema. Estes rexistros permiten a detección de actividades sospeitosas, a resolución de problemas de seguridade e o cumprimento de regulamentos e políticas de seguridade.

Software e sistemas comúns para auditoría:

Windows: En sistemas Windows, o Servizo de Auditoría de Seguridade (Security Audit Service) permite a rexistración de eventos de seguridade no sistema. As ferramentas como o Visor de eventos permiten analizar os rexistros de auditoría e identificar problemas de seguridade.

Linux: En sistemas Linux, as auditorías se rexistran en “log” do sistema clasificados por ferramentas como rsyslogd ou auditd. Estes rexistros poden ser analizados con ferramentas como AIDE ou Splunk para identificar posibles problemas de seguridade.

Rsyslogd permite enviar todos os eventos a un servidor central de análise de logs.

Sistemas de Cifrado

O cifrado é un proceso fundamental que implica a conversión de datos ou información nun formato ilexible e incomprensible para que só as persoas autorizadas poidan acceder a ela. Este proceso é esencial para garantir a seguridade e a confidencialidade dos datos durante a súa transmisión e almacenamento en sistemas informáticos.

O principal obxectivo do cifrado é protexer a información sensible contra accesos non autorizados, evitando que terceiros non autorizados poidan ler ou entender os datos protexidos. Ao cifrar os datos, mesmo se unha persoa ou entidade non autorizada accede a eles, non poderán interpretalos sen a clave de cifrado adecuada.

Ademais de garantir a confidencialidade dos datos, o cifrado tamén pode axudar a protexer a integridade e a autenticidade dos datos, asegurando que non foron alterados ou manipulados durante a súa transmisión ou almacenamento.

Os mecanismos de cifrado existentes podemos clasificalos en :

- **Cifrado Simétrico**: No cifrado simétrico se emprega unha única chave para cifrar e descifrar. A chave de cifrado debe ser coñecida únicamente para as partes que se comunican. O punto débil neste sistema e a comunicación da chave de cifrado a outra parte.

  Os algoritmos máis utilizados son AES e DES. O DES é vulnerable e está substituíndose por 3DES, que é lento. Polo que o recomendado é AES. Outros algoritmos son RC4 (que se usa en TLS e para cifrado de arquivos) e RC5

- **Cifrado Asimétrico** : Utiliza un par de chaves distintas para cifrar e descifrar a información. Cada clave dun par (chamadas chave pública e chave privada) é matematicamente relacionada, pero unha clave só pode cifrar datos e a outra só pode descifralos. A chave pública pode ser compartida libremente, mentres que a chave privada debe ser mantida en segredo polo seu dono, eliminando polo tanto o problema de distribución da chave.

  O seu punto crítico e o garantir a autenticidade da chave pública, para o que se utilizan mecanismos como a firma de autoridades de certificación ou cadeas de confianza.

- **Cifrado de Sentido Único**: Tamén coñecido como función de hash, é unha técnica criptográfica na que se toma unha entrada de datos (como unha mensaxe ou unha contrasinal) e se aplica un algoritmo de hash para producir unha saída única e fixa de tamaño fixo. Esta saída de datos non pode ser retrocedida ou descifrada para obter a entrada orixinal. Aínda que é posíbel calcular o hash dende a entrada, non é posíbel determinar a entrada orixinal dende o hash. A principal utilidade do cifrado de sentido único reside na súa capacidade para almacenar e comparar información de forma segura sen necesidade de almacenar a entrada orixinal. Algúns exemplos de aplicacións do cifrado de sentido único inclúen:

  - Almacenamento Seguro de Contrasinais: Os servidores de autenticación almacenan xeralmente non as contrasinais dos usuarios, senón os hashes das contrasinais. Cando un usuario intenta acceder ao sistema, a súa contrasinal é hashada e comparada co hash almacenado. Isto protexe as contrasinais dos usuarios mesmo en caso de acceso non autorizado ao sistema.

    - Verificación de Integridade de Datos: Os hashes tamén se utilizan para verificar a integridade de datos. Se os datos orixinais cambian, o hash resultante tamén cambiará. Isto permítelle aos usuarios verificar se os datos foron alterados durante a transmisión ou o almacenamento.
    - Xestión de Chaves Criptográficas: Os hashes tamén se utilizan para xerar resumos únicos e fixos de chaves criptográficas. Estes resumos poden axudar a identificar e verificar as chaves sen necesidade de almacenar as chaves orixinais.

Si queremos garantir a confidencialidade da información dos nosos dispositivos debemos recurrir ao cifrado, que pode ser:

- A nivel de carpeta: Se cifra todo o contido dunha carpeta, pero tanto o sistema de arquivos como o resto do disco están accesibles para todo o mundo.
- A nivel de dispositivo: Se cifra un dispositivo completo, non se pode ter coñecemento nin siquera das particións ou sistemas de arquivos que emprega o dispositivo.

O TPM

O Trusted Platform Module (TPM) é un chip de seguridade hardware que está integrado en placas base de ordenadores e dispositivos electrónicos. O seu obxectivo principal é proporcionar unha plataforma segura para a xestión de chaves criptográficas, a autenticación e a protección de datos sensibles.

Obxectivos do TPM:

- **Protexer as Chaves Criptográficas**: O TPM almacena chaves criptográficas de forma segura e realiza operacións criptográficas, como cifrado e descifrado, de forma segura no seu interior. Isto axuda a protexer as chaves de cifrado de posibles ataques físicos ou software malicioso.
- **Autenticación do Dispositivo**: O TPM permite a autenticación segura do dispositivo, garantindo que o hardware non foi alterado ou comprometido. Isto é especialmente importante en entornos nos que a confianza no dispositivo é fundamental, como na autenticación en sistemas de seguridade ou en acceso a redes corporativas.
- **Integridade do Sistema**: O TPM proporciona unha maneira de verificar a integridade do sistema, asegurando que o software e o firmware non foron modificados ou comprometidos. Isto axuda a detectar calquera tentativa de intrusión ou infección por malware no sistema.
- **Protección de Datos Sensibles**: O TPM pode ser utilizado para cifrar e protexer datos sensibles almacenados no dispositivo. Isto garante que os datos só poidan ser accedidos e descifrados por usuarios autorizados, axudando a previr a fuga de información ou o acceso non autorizado aos datos.
- **Xestión de Identidade e Credenciais**: O TPM pode ser utilizado para almacenar e xestionar credenciais de usuario, como contrasinais ou certificados dixitais, de forma segura. Isto permite a autenticación segura dos usuarios e axuda a protexer as súas credenciais de posibles ataques de roubo ou intrusión.

A comunicación segura: Cifrado e Firma Dixitais.

Hoxe en día e imprescindible garantir tanto a privacidade da información que se intercambia nas redes como o non repudio, de xeito que esteamos seguros da orixe da información que nos chega e do destino da información que enviamos.

Toda esta seguridade se implanta en torno ao cifrado asimétrico. Como xa explicamos, a debilidade do cifrado asimétrico está en garantir que a chave pública é auténtica, que pertence a quen dice pertencer. Para ese obxectivo se empregan dúas estratexias diferenciadas:

- Descentralizada ou de cadeas de confianza: Os integrantes das comunicacións se aseguran persoalmente da lexitimidade das chaves públicas e as firman dixitalmente para que outros saiban que poden fiarse. Si nos fiamos de un membro tamén nos fiaremos de todos os membros de que este se fíe. E o mecanismo usado por PGP, e é moi usada no e-mail
- Centralizada ou de autoridades certificadoras: Se concede a un conxunto reducido de entidades constituídas legalmente a potestade de examinar e garantizar mediante firma dixital a autenticidade das chaves públicas. E o mecanismo de certificación X509 utilizado en https e prácticamente en todos os servizos de internet.

Un ***certificado*** e un documento que contén información sobre a entidade certificada xunto coa súa chave pública, e unha firma dixital que asegura a súa veracidade.

O cifrado de chave pública está enfocado en dúas operacións:

FIRMA: A firma pretende garantir a autenticidade e procedencia dun documento, impedindo a súa manipulación sin ser detectada. O mecanismo e o seguinte:

- Se crea un “hash” do documento a firmar
- Se cifra o “hash” coa chave privada do firmante (firma)
- Se adxunta o “hash” cifrado ao documento

O destinatario poderá descifrar o “hash” coa chave pública do firmante e verificar a autenticidade do documento.

CIFRADO: O cifrado pretende garantir a confidencialidade da información transmitida. O mecanismo é o seguinte:

- Se crea unha chave de cifrado simétrica ao azar
- Se cifra o documento
- Se cifra a chave de cifrado empregada coa chave pública do destinatario
- Se adxunta a chave de cifrado cifrada ao documento.

O destinatario poderá descifrar a chave de cifrado coa súa chave privada e descifrar o documento

A firma e o cifrado son a base do protocolo https imprescindible hoxe en día na www. Cando un cliente http (Chrome, Mozilla...) quere unha páxina mediante https, a secuencia é a seguinte:

- O navegador realiza a petición https://
- O servidor contesta co seu certificado, que contén a información relevante do sitio web xunto coa súa chave pública.

- O navegador comproba o certificado e a súa firma coas chaves públicas das entidades certificadoras das que dispón e opcionalmente comprobando a validez do certificado no servidor de certificación. Si a comprobación non é correcta se emite unha alerta.
- O navegaro crea unha chave de cifrado simétrica ao azar, e a firma coa chave pública do certificado recibido enviándoa ao servidor.
- O servidor descifra a chave simétrica e a utiliza para cifrar toda a información que se intercambie no futuro co cliente.

Deste xeito garantimos a autenticidade do servidor (porque ten a chave privada dunha chave pública garantizada por unha autoridade de certificación aceptada por nos), a confidencialidade (porque a información vai cifrada) e a integridade (ningún intermediario poderá modificar a información sin ser detectado).

Tanto a www como o e-mail son mecanismos de comunicación baseados en texto claro altamente inseguros, que deberían ser protexidos mediante firma e cifrado.

Mecanismos de seguridade Pasiva

A seguridade pasiva é un enfoque na protección e prevención de riscos ou ameazas que en lugar de tomar medidas activas encamiñadas a impedir o impacto dun ataque, se enfocan en tomar medidas preventivas para minimizar ou eliminar o seu impacto. Se trata de implementar medidas preventivas protexendo os sistemas e recursos de forma proactiva. Algúns exemplos son:

- Vigilancia por Cámaras de Seguridade
- Iluminación Exterior Automatizada
- Filtros de Correo Electrónico Antispam
- Fechaduras Electrónicas en Portas:
- Copias de Seguridade

As copias de Seguridade (Backups)

Os backups son unha parte fundamental da xestión da información e da seguridade dos datos nunha organización ou para usuarios individuais. A súa importancia radica en:

- Protección de Datos: Os backups axudan a protexer os datos contra a perda debido a fallos de hardware, erro humano, ataque de malware ou desastres naturais.
- Recuperación de Datos: Permítennos restaurar os datos a un estado anterior en caso de perda ou corrupción dos datos orixinais.
- Continuidade do Negocio: Unha adecuada estratexia de copias de seguridade pode axudar a minimizar o impacto dunha interrupción do negocio, permitindo unha rápida recuperación das operacións.

Existen varios **tipos de backups,** incluíndo:

- **Completo**: Faise unha copia de seguridade de todos os datos seleccionados.
- **Incremental**: Só se copian os datos que cambiaron ou foron engadidos desde o último backup.

- **Diferencial**: Copia todos os datos que cambiaron desde o último backup completo.

As copias de seguridade precisan de:

- **Planificación**: Define unha política de copias de seguridade que inclúa a frecuencia dos backups, os tipos de backups e os datos a copiar.
- **Selección de Datos**: Identifica os datos críticos e sensibles que requiren copias de seguridade regulares.
- **Almacenamento Seguro:** Mantén as copias de seguridade nun lugar seguro, lonxe do hardware principal e protexido contra acceso non autorizado.
- **Automatización**: Utiliza ferramentas de copia de seguridade automáticas para asegurar que os backups se realicen regularmente e sen erro humano.
- **Probas de Restauración**: Realiza probas regulares de restauración para comprobar que os backups se poden recuperar correctamente e que os datos se restauran correctamente.
- **Diversificación de Localización**: Mantén copias de seguridade en varios lugares físicos ou en nube para protexelos contra desastres locais.

Unha boa práctica en canto as copias de seguridade é a **estratexia 3-2-1:**

- **3 -** Se deben manter 3 copias de calqueira información importante: Os datos orixinais e 2 backups
- **2 –** As copias deben estar almacenadas en 2 soportes distintos (distintas tecnoloxías) de almacenamento.
- **1 –** Unha das copias de seguridade debe estar deslocalizada fora da localización habitual (offsite)

Tamén e imprescindible que os backups sexan AUTOMÁTICOS, non poden depender da dispoñibilidade do persoal para ser realizados.

Existen varias ferramentas de software dispoñibles para axudar a xestionar e automatizar o proceso de copias de seguridade, incluíndo Acronis Backup, Backup Exec de Veritas, Bacula (Multiplataforma) ou o sistema de Copia de Seguridade de Windows (Windows Backup)

Seguridade Perimetral

A seguridade perimetral é unha estratexia de seguridade informática que se enfoca en protexer a rede dunha organización desde o seu perímetro externo contra ameazas e intrusións. Esta estratexia implica a implementación de varias capas de defensa (defensa en profundidade) para protexer a rede e os sistemas internos contra ameazas externas. Algúns dos conceptos clave na seguridade perimetral inclúen:

1. DMZ (Zona Desmilitarizada):

A DMZ é unha rede intermedia situada entre a rede interna dunha organización e a Internet. É unha área semiprotexida onde se colocan servidores e servizos que requiren acceso desde a Internet, como servidores web ou servidores de correo electrónico. A DMZ actúa como unha barreira adicional entre a rede interna e a Internet, protexendo os sistemas internos de posibles ataques.

2. Firewall:

O firewall é unha peza fundamental da seguridade perimetral que controla o tráfico de rede entre a rede interna e externa. Hai varios tipos de firewalls, incluíndo:

Firewall de Rede: Opera a nivel de rede e filtra o tráfico baseado en enderezos IP, portas e protocolos.

Firewall de Aplicacións: Monitoriza o tráfico de aplicacións e filtra o tráfico baseado en contido e comportamento.

3. Defensa en Profundidade:

A defensa en profundidade é unha estratexia de seguridade que implica a implementación de múltiples capas de seguridade en diferentes niveis da infraestrutura de rede. Esta estratexia ten como obxectivo proporcionar unha protección máis robusta contra ameazas e intrusións. Algúns exemplos de medidas de defensa en profundidade inclúen:

Control de Acceso a Rede: Limita o acceso á rede só a usuarios autorizados.

Cifrado de Datos: Protexe os datos confidenciais durante a transmisión e almacenamento.

Monitorización e Xestión de Vulnerabilidades: Identifica e aborda as vulnerabilidades de seguridade na rede e nos sistemas.

PortKnocking e SPA

El Port Knocking e o SPA (Single Packet Authorization) son técnicas de seguridad utilizadas para ocultar o proteger el acceso a servicios de red, como puertos de un servidor, de manera que solo aquellos que conozcan el "secreto" adecuado puedan acceder a ellos. A

Port Knocking:

O Port Knocking é unha técnica de seguridade que consiste en enviar unha secuencia específica de solicitudes ou paquetes a un servidor para abrir portas específicas que, de outro xeito, estarían pechadas. Esta secuencia de paquetes é como un "toque" na porta do servidor que só se abre cando se recibe a secuencia correcta. Unha vez que o servidor detecta a secuencia correcta de "toques", abra as portas desexadas para permitir o acceso ao servicio.

Funcionamento: O Port Knocking pode ser implementado a través de scripts personalizados ou software específico que monitora os paquetes de rede que chegan ao servidor. Cando o servidor detecta a secuencia específica de paquetes que forman o "toque", executa unha acción para abrir as portas desexadas durante un período de tempo determinado.

Single Packet Authorization (SPA):

O Single Packet Authorization (SPA) é outra técnica de seguridade que permite abrir portas en un servidor mediante o envío dun único paquete de rede. O SPA require que o cliente envíe un paquete especial coas credenciais e a información de autorización necesarias para acceder ao servidor.

Funcionamento: Cando o servidor recibe o único paquete de autorización, verifica a información contida no paquete e, se é válida, abre as portas especificadas durante un período de tempo limitado para permitir o acceso ao cliente. O SPA é atractivo porque reduce a exposición do servidor a ataques de forza bruta ou escaneos de portas.

En Linux fwknop ofrece un sistema bastante fiable de SPA.

Servizos de Acceso Remoto

Os servizos de acceso remoto son ferramentas fundamentais para permitir que os usuarios se conecten e accedan a recursos de rede desde localizacións remotas de forma segura.

1. **SSH (Secure Shell):**

SSH é un protocolo de rede que permite aos usuarios conectarse de forma segura a un servidor remoto a través dunha conexión encriptada. Proporciona unha conexión segura para a administración remota de sistemas e transferencia segura de arquivos.

2. **Túneles SSH:**

Os túneles SSH permiten crear conexións seguras entre dous sistemas a través dun servidor intermedio. Isto conséguese redireccionando o tráfico a través dunha conexión SSH encriptada. Os túneles SSH poden utilizarse para acceder a servizos internos dunha rede desde fóra, protexer o tráfico de rede en conexións inseguras ou evitar restricións de rede. Para crear un túnel SSH, podes utilizar o comando ssh con opcións de redireccionamento de portos, como -L para redireccionamento local ou -R para redireccionamento remoto.

3. Proxy SOCKS SSH:

Un proxy SOCKS SSH é un servidor proxy que utiliza unha conexión SSH para enrutar o tráfico de rede de forma segura a través dunha rede remota. Este tipo de proxy proporciona unha capa adicional de seguridade ao cifrar o tráfico de rede entre o cliente e o servidor proxy. Podes configurar un proxy SOCKS SSH no teu cliente SSH para enrutar todo o tráfico de rede a través dunha conexión SSH.

4. VPN

Unha VPN (Rede Privada Virtual) é unha tecnoloxía que permite crear unha conexión segura e cifrada entre dispositivos ou redes a través dunha rede pública, como Internet. As VPNs son amplamente utilizadas para garantir a privacidade e a seguridade das comunicacións en liña, así como para acceder a recursos de rede de forma remota.

Unha VPN crea unha "túnel" seguro e cifrado entre o dispositivo cliente e o servidor VPN, a través do cal todo o tráfico de rede se transmite de forma segura. Isto protexe os datos que se transmiten na rede pública de seren espiados ou interceptados por terceiros. As VPNs tamén permiten ocultar o enderezo IP real do dispositivo cliente, proporcionando anonimato e privacidade en liña.

Mediante unha VPN podemos conectar un equipo remoto a unha rede ou dúas redes entre sí de xeito que se poderá traballar como si estiveran na mesma localización, facendo que todas as partes se unan na mesma rede.