**CYBERYOUTH**

**Formazione non formale per la sicurezza informatica e la resilienza delle organizzazioni giovanili e dei giovani**

***Accademia online***

***per la cybersecurity dei giovani***

****

**Implementazione delle Soluzioni di Sicurezza**

Indice

[Introduzione](#_heading=h.fpb3yt6tcffi)

[Cosa imparerai](#_heading=h.bd1t10x6k115)

[Perché è importante e come potrà aiutarti nella vita di tutti i giorni](#_heading=h.1fqj6c1n3ygs)

[Che carriera potrai intraprendere](#_heading=h.l25siuf1d90q)

[Pre-requisiti](#_heading=h.obikvf4haym5)

[Materiale](#_heading=h.snpqznqbwxs)

[4.1 Secure Protocols](#_heading=h.2yz7x8bu8zb5)

[HTTPS](#_heading=h.mr2hcuf317tb)

[SSH](#_heading=h.x4bvrqwuw8js)

[LDAPS](#_heading=h.lovf4p6u7t0d)

[SSL\TSL](#_heading=h.xg04l0g235rx)

[SNMP](#_heading=h.g4p0ycyz9c21)

[IPsec](#_heading=h.5cvpgyivdyn7)

[Kerberos](#_heading=h.jld6kiliae8p)

[Conclusioni](#_heading=h.xw8j0ql8ygt1)

[4.2 Soluzioni per la Sicurezza delle Applicazioni](#_heading=h.fm56f6motz39)

[Endpoint Protection](#_heading=h.6qpu0sb9n7a4)

[Endpoint Protection Platforms (EPP)](#_heading=h.m4fkwrzqoln)

[Endpoint Detection & Response (EDR)](#_heading=h.hydkmwexfn2)

[Extended Detection & Response (XDR)](#_heading=h.sfet32tqxln5)

[Database Protection](#_heading=h.vigzv62c4b25)

[Data Discovery and Classification.](#_heading=h.550yty1wqxp)

[Intrusion Detection & Prevention Systems](#_heading=h.513chn51g6ea)

[(IDPS)](#_heading=h.trq7iiezrcjn)

[Funzioni Base di un IDPS](#_heading=h.owth8i9wxnz)

[Security Information and Event Management](#_heading=h.nmqkk5yo33w5)

[(SIEM)](#_heading=h.ylwkyis1jooy)

[Data Loss Prevention (DLP)](#_heading=h.a6rmc9vx6o1)

[Application Security](#_heading=h.x17z5ggnarq)

[Code Review](#_heading=h.t38ren4sf7wa)

[Software Composition Analysis (SCA)](#_heading=h.59oj4z7qu6au)

[Static Application Security Testing (SAST)](#_heading=h.pp92kiybhher)

[Dynamic Application Security Testing (DAST)](#_heading=h.npqyi5bjmwfr)

[Interactive Application Security Testing (IAST)](#_heading=h.cfk25eh0dl6a)

[Conclusioni](#_heading=h.m7quy8g9mit)

[4.3 Secure Network Design](#_heading=h.3o186oib6p8o)

[Network Segmentation](#_heading=h.4yf42v7v3mq5)

[Conclusioni](#_heading=h.ykfi7c3wyyt3)

[4.4 Secure Cloud Controls & Solutions](#_heading=h.bx698qd91bm4)

[Cloud Security Controls](#_heading=h.wfku2zhkei9q)

[Conclusioni](#_heading=h.s9qb5yxkl8lb)

[L’angolo del Geek](#_heading=h.abdmhrml8t9n)

[Conclusioni](#_heading=h.8r62o9nqh7h)

[Quiz](#_heading=h.5rdrustk5rg8)

# 

# Introduzione

## Cosa imparerai

In questa unità, imparerai vari controlli e soluzioni di sicurezza che sono parametri implementati per proteggere varie forme di dati e infrastrutture importanti per un'organizzazione, che vanno dalle scelte chiave di progettazione, architettura e implementazione fatte dalle organizzazioni per soddisfare i requisiti di sicurezza specificati per sistemi o componenti di sistema.

## Perché è importante e come potrà aiutarti nella vita di tutti i giorni

Questo modulo è essenziale per te e per la tua organizzazione poiché l'implementazione di soluzioni di sicurezza è importante in quanto diventano parte integrante di qualsiasi operazione legata ai dati per organizzazioni e individui di tutte le dimensioni e settori. Un programma robusto di sicurezza dell'informazione aiuta a proteggere i tuoi asset tecnologici e lo spazio fisico da attacchi maligni dall'esterno e dall'interno della tua organizzazione. Queste sono importanti soluzioni di sicurezza per mantenere te, i tuoi dipendenti e l'infrastruttura fisica al sicuro da danni difendendo i tuoi dati e le informazioni critiche della tua azienda da hacker e da altre minacce alla sicurezza informatica. Ciò include dati sensibili, informazioni personalmente identificabili (PII), informazioni sanitarie protette (PHI), informazioni personali, proprietà intellettuale, dati e sistemi informativi governativi e industriali. Ti consente anche di rimanere conforme alle leggi e ai regolamenti aggiornati nel tuo paese o nella tua regione.

## Che carriera potrai intraprendere

Esistono diverse opzioni di carriera che puoi intraprendere nel campo della sicurezza, tra le più importanti:

* Ingegnere della sicurezza, che lavora per mantenere i sistemi di sicurezza di individui e organizzazioni operativi, implementando e testando nuove funzionalità di sicurezza, pianificando aggiornamenti di computer e reti, risolvendo problemi, rispondendo a incidenti di sicurezza e molti altri.
* Ingegnere della sicurezza delle applicazioni, che lavora per anticipare le vulnerabilità strutturali e determinare come correggerle. Il loro lavoro include l'aggiornamento del software, la creazione di firewall e l'esecuzione di programmi di crittografia all'interno di una rete informatica o di un'applicazione.
* Cloud Engineer/Architect, che lavora per aggiornare i sistemi basati su cloud per migliorare le operazioni e proteggersi da violazioni di dati e minacce alla sicurezza informatica, risolvendo problemi reali o potenziali con le piattaforme di cloud computing, fornendo servizi di supporto cloud necessari che aiutano individui e aziende a utilizzare le applicazioni in nuovi modi.

## 

## Pre-requisiti

In generale, un ingegnere della sicurezza o un architetto cloud deve avere le seguenti qualifiche:

* Laurea in Informatica, IT, Ingegneria dei Sistemi o un campo simile
* Due anni di esperienza lavorativa in mansioni correlate alla sicurezza informatica come rilevamento e risposta agli incidenti e informatica forense
* Esperienza con la funzionalità, il funzionamento e la manutenzione di firewall e varie forme di sicurezza degli endpoint
* Competenza in linguaggi/strumenti come C++, Java, Node, Python, Ruby, Go o Power Shell
* Capacità di lavorare in un ambiente ad alta velocità, spesso sotto pressione
* Possedere l'occhio giusto per il dettaglio e notevoli capacità di risoluzione dei problemi
* Conoscenza aggiornata sulle ultime tendenze della sicurezza informatica e tattiche degli hacker.

Si noti che diverse organizzazioni possono avere più o meno qualifiche o attribuire maggiore o minore importanza a uno qualsiasi dei criteri indicati.

## Materiale

## 

## 

## 4[.1 Secure Protocols](https://docs.google.com/document/d/1r9tAENn4JvJzvoSJP-L_gPrG4BwmCnxY/edit#heading=h.2yz7x8bu8zb5)

## 

## [HTTPS](https://docs.google.com/document/d/1r9tAENn4JvJzvoSJP-L_gPrG4BwmCnxY/edit" \l "heading=h.2yz7x8bu8zb5)

Hypertext Transfer Protocol Secure (HTTPS) è la versione sicura di HTTP, che è il protocollo primario utilizzato per inviare dati tra un browser web e un sito web. HTTPS è crittografato al fine di aumentare la sicurezza del trasferimento dei dati. Questo è particolarmente importante quando gli utenti trasmettono dati sensibili, ad esempio accedendo a un conto bancario, a un servizio di posta elettronica o a un fornitore di assicurazioni sanitarie.

Qualsiasi sito web, specialmente quelli che richiedono credenziali di accesso, dovrebbe utilizzare HTTPS. Nei browser web moderni come Chrome, i siti web che non utilizzano HTTPS sono contrassegnati in modo diverso rispetto a quelli che lo fanno. Cerca un lucchetto nella barra degli indirizzi URL per indicare che la pagina web è sicura. I browser web prendono HTTPS molto sul serio; Google Chrome e altri browser contrassegnano tutti i siti web non in HTTPS come non sicuri.

## SSH

SSH o Secure Shell è un protocollo di comunicazione di rete che consente a due computer di comunicare (cf. http o protocollo di trasferimento di ipertesto, che è il protocollo utilizzato per il trasferimento di ipertesto come pagine web) e condividere dati. Una caratteristica intrinseca di SSH è che la comunicazione tra i due computer è crittografata, il che significa che è adatta all'uso su reti non sicure.

SSH viene spesso utilizzato per "effettuare il login" e eseguire operazioni su computer remoti, ma può anche essere utilizzato per il trasferimento di dati.

**Come si utilizza SSH?**

Si utilizza un programma sul proprio computer (client SSH) per connettersi al nostro servizio (server) e trasferire i dati da e verso il nostro archivio utilizzando un'interfaccia utente grafica o una riga di comando. Sono disponibili molti programmi che consentono di effettuare questo tipo di trasferimento e alcuni sistemi operativi come Mac OS X e Linux hanno questa capacità integrata.

## LDAPS

Il Lightweight Directory Access Protocol (LDAP) è un protocollo che consente alle applicazioni di interrogare rapidamente le informazioni sugli utenti.

Le aziende memorizzano nomi utente, password, indirizzi email, connessioni alle stampanti e altre informazioni statiche all'interno dei directory. LDAP è un protocollo applicativo aperto e neutrale rispetto ai fornitori che consente di accedere e gestire questi dati. LDAP può gestire anche l'autenticazione, consentendo agli utenti di effettuare l'accesso una sola volta e accedere a molti file diversi sul server.

LDAP è un protocollo e non specifica come funzionano i programmi di directory. È piuttosto una forma di linguaggio che consente agli utenti di trovare le informazioni di cui hanno bisogno molto rapidamente. LDAP è neutrale rispetto ai fornitori, quindi può essere utilizzato con una varietà di programmi di directory diversi. Tipicamente, un directory contiene dati che sono:

- Descrittivi. Diversi punti, come il nome e la posizione, si uniscono per definire un'entità.

- Statici. Le informazioni cambiano poco e, quando lo fanno, le modifiche sono sottili.

- Preziosi. I dati memorizzati nel directory sono fondamentali per le funzioni aziendali principali ed è un elemento toccato più volte.

A volte, le persone utilizzano LDAP in combinazione con altri sistemi durante la giornata lavorativa. Ad esempio, i dipendenti possono utilizzare LDAP per connettersi alle stampanti o verificare le password. Questi dipendenti possono poi passare a Google per l'email, che non si basa affatto su LDAP.

## SSL\TSL

SSL, o Secure Sockets Layer, è un protocollo di sicurezza su Internet basato su crittografia. È stato sviluppato per la prima volta da Netscape nel 1995 con lo scopo di garantire la privacy, l'autenticazione e l'integrità dei dati nelle comunicazioni su Internet. SSL è il predecessore dell'attuale crittografia TLS utilizzata oggi.

Un sito web che implementa SSL/TLS ha "HTTPS" nella sua URL invece di "HTTP".

Transport Layer Security, o TLS, è un protocollo di sicurezza ampiamente adottato progettato per agevolare la privacy e la sicurezza dei dati nelle comunicazioni su Internet. Un caso d'uso principale di TLS è la crittografia della comunicazione tra applicazioni web e server, come i browser web che caricano un sito web. TLS può essere utilizzato anche per crittografare altre comunicazioni come l'email, la messaggistica e la voce su IP (VoIP).

**Qual è la differenza tra TLS e SSL?**

TLS è evoluto da un precedente protocollo di crittografia chiamato Secure Sockets Layer (SSL), sviluppato da Netscape. La versione 1.0 di TLS è iniziata come versione 3.1 di SSL, ma il nome del protocollo è stato cambiato prima della pubblicazione per indicare che non era più associato a Netscape. A causa di questa storia, i termini TLS e SSL vengono talvolta usati in modo interscambiabile.

## SNMP

Simple Network Management Protocol (SNMP) è un protocollo di livello applicativo per il monitoraggio e la gestione di dispositivi di rete in una rete locale (LAN) o una rete estesa (WAN). Lo scopo di SNMP è fornire ai dispositivi di rete, come router, server e stampanti, un linguaggio comune per la condivisione di informazioni all'interno di un Sistema di Gestione di Rete (NMS).

L'architettura client-server di SNMP è composta dai seguenti tre componenti:

- Gestore SNMP

- Agente SNMP

- Base di Informazioni di Gestione (MIB).

Il gestore SNMP agisce come client, l'agente SNMP agisce come server e il MIB funge da database del server. Quando il gestore SNMP pone una domanda all'agente, quest'ultimo utilizza il MIB per fornire la risposta.

SNMP è così diffuso che la maggior parte dei dispositivi di rete è pre-confezionata con agenti SNMP. Tuttavia, per utilizzare il protocollo, gli amministratori di rete devono prima modificare le impostazioni di configurazione predefinite dei loro dispositivi di rete in modo che gli agenti SNMP possano comunicare con il sistema di gestione di rete della rete.

SNMP fa parte della suite originale del Protocollo Internet (IP) come definito dall'Internet Engineering Task Force (IETF). Esistono diverse versioni del protocollo SNMP. La versione più recente, SNMPv3, include meccanismi di sicurezza per l'autenticazione, la crittografia e il controllo degli accessi.

## IPsec

**Cos'è IPsec?**

IPsec è un gruppo di protocolli per la sicurezza delle connessioni tra dispositivi. IPsec aiuta a mantenere sicuri i dati inviati su reti pubbliche. È spesso utilizzato per configurare VPN e funziona crittografando i pacchetti IP, insieme all'autenticazione della fonte da cui provengono i pacchetti.

Nel termine "IPsec", "IP" sta per "Internet Protocol" e "sec" per "sicuro". Il Protocollo Internet è il principale protocollo di routing utilizzato su Internet; esso designa dove i dati andranno utilizzando gli indirizzi IP. IPsec è sicuro perché aggiunge crittografia e autenticazione a questo processo.

**Perché è importante IPsec?**

I protocolli di sicurezza come IPsec sono necessari perché i metodi di networking non sono crittografati per impostazione predefinita.

Quando si invia posta attraverso un servizio postale, una persona di solito non scrive il proprio messaggio all'esterno della busta. Invece, chiude il messaggio all'interno della busta in modo che nessuno che gestisce la posta tra mittente e destinatario possa leggere il messaggio. Tuttavia, le suite di protocolli di networking come TCP/IP si occupano solo della connessione e della consegna, e i messaggi inviati non sono nascosti. Chiunque si trovi in mezzo può leggerli. IPsec e altri protocolli che crittografano i dati mettono essenzialmente una busta attorno ai dati mentre attraversano le reti, mantenendoli al sicuro.

## [Kerberos](https://docs.google.com/document/d/1r9tAENn4JvJzvoSJP-L_gPrG4BwmCnxY/edit" \l "heading=h.2yz7x8bu8zb5)

Kerberos fornisce un server di autenticazione centralizzato il cui compito è autenticare gli utenti verso i server e i server verso gli utenti. Nell'autenticazione di Kerberos, viene utilizzato un server di autenticazione e un database per l'autenticazione del client. Kerberos funziona come un server di terze parti fidato noto come Key Distribution Center (KDC). Ogni utente e servizio sulla rete è un principale.

I principali componenti di Kerberos sono:

Server di autenticazione (AS): il server di autenticazione effettua l'autenticazione iniziale e rilascia un biglietto per il Ticket Granting Service.

Database: il server di autenticazione verifica i diritti di accesso degli utenti nel database.

Server Ticket Granting (TGS): il server Ticket Granting rilascia il biglietto per il server.

## Conclusioni

Security controls and solutions are critical subjects which continuously develop to reach the highest security level, where organisations become more aware of its importance with the fast paced technological developments and related security concerns. Security solutions provided by the experts are subjected to be more important in this sense where efforts to produce satisfying security requirements for systems will continue playing critical roles to protect various forms of data and infrastructure.

# 

# 4[.2](https://docs.google.com/document/d/1r9tAENn4JvJzvoSJP-L_gPrG4BwmCnxY/edit#heading=h.wv8lmqsplpdd) Soluzioni per la Sicurezza delle Applicazioni

# 

# Endpoint Protection

# 

# Endpoint Protection Platforms (EPP)

La protezione degli endpoint fornisce una sicurezza essenziale per molti tipi di endpoint, dai telefoni intelligenti alle stampanti. Una piattaforma di protezione degli endpoint (EPP) è una suite integrata di tecnologie di protezione degli endpoint, come antivirus, crittografia dei dati, prevenzione delle intrusioni e prevenzione della perdita dei dati, che rà rilevare ed arrestare una varietà di minacce all'endpoint.

Una piattaforma di protezione degli endpoint fornisce un quadro per la condivisione dei dati tra le tecnologie di protezione degli endpoint. Questo fornisce un approccio più efficace rispetto a una raczione di prodotti di sicurezza isolati che mancano della capacità di comunicare.

Il volume e la complessità degli attacchi informatici sono in aumento, e i sistemi di tecnologia dell'informazione (IT) e i dati sono costantemente sotto minaccia di attacco. Gli attacchi informatici sono diventati sempre più complessi, utilizzando tecniche multiple e coordinate per infiltrarsi nei sistemi IT di un'organizzazione. Gli endpoint sono spesso la porta attraverso cui gli aggressori ottengono l'accesso iniziale.

## Endpoint Detection & Response (EDR)

La rilevazione e risposta sugli endpoint (EDR), nota anche come rilevazione e risposta alle minacce sugli endpoint (ETDR), è una soluzione integrata di sicurezza degli endpoint che combina il monitoraggio continuo in tempo reale e la raccolta di dati dagli endpoint con capacità di risposta e analisi automatizzate basate su regole. Il termine è stato suggerito da Anton Chuvakin di Gartner per descrivere i sistemi di sicurezza emergenti che rilevano e investigano attività sospette su host ed endpoint, impiegando un alto grado di automazione per consentire ai team di sicurezza di identificare e rispondere rapidamente alle minacce.

Le funzioni principali di un sistema di sicurezza EDR sono:

1. Monitorare e raccogliere dati sull'attività dagli endpoint che potrebbero indicare una minaccia.

2. Analizzare questi dati per identificare pattern di minaccia.

3. Rispondere automaticamente alle minacce identificate per rimuoverle o contenerle e notificare al personale della sicurezza.

4. Strumenti di analisi e forensica per ricercare le minacce identificate e cercare attività sospette.

## Extended Detection & Response (XDR)

Secondo la società di analisi Gartner, Extended Detection and Response (XDR) è "uno strumento basato su SaaS (Software as a Service), specifico del fornitore, per la rilevazione delle minacce alla sicurezza e la risposta agli incidenti, che integra nativamente più prodotti di sicurezza in un sistema operativo di sicurezza coerente che unifica tutti i componenti con licenza."

XDR consente a un'azienda di andare oltre i controlli tipici di rilevamento, fornendo una visione olistica e allo stesso tempo più semplice delle minacce in tutto il panorama tecnologico. XDR fornisce informazioni sulle minacce attuabili in tempo reale alle operazioni di sicurezza per risultati migliori e più veloci.

I principali vantaggi di Extended Detection and Response (XDR) sono:

- Migliorate capacità di protezione, rilevamento e risposta.

- Miglioramento della produttività del personale della sicurezza operativa.

- Riduzione del costo totale di proprietà per una rilevazione ed una risposta efficace alle minacce alla sicurezza.

Extended Detection and Response (XDR) promette di consolidare più prodotti in una piattaforma unificata per la rilevazione e la risposta agli incidenti di sicurezza. XDR rappresenta una logica evoluzione delle soluzioni di rilevazione e risposta agli endpoint (EDR) in uno strumento primario per la risposta agli incidenti.

## Database Protection

## Data Discovery and Classification.

La scoperta dei dati e la classificazione dei dati sono due processi separati, ma lavorano insieme per fornire alla tua organizzazione una visione completa dei dati in tutto l'ambiente. Prima di vedere come lavorano insieme, diamo una breve definizione di ciascuno.

**Scoperta dei dati**

La scoperta dei dati è il processo di scansione dell'intero ambiente per trovare ed identificare dove risiedono i dati strutturati e non strutturati in tutta l'azienda. Ciò significa guardare su tutta la rete, compresi i server di file e l'hardware, per determinare dove risiedono i dati sensibili e regolamentati.

In sostanza, la scoperta dei dati consente alle aziende di identificare, classificare e tracciare i dati sensibili in modo che abbiano una visione completa di dove risiedono i loro dati. Questo aiuta le aziende a proteggere meglio i loro dati e ad assicurarsi di rispettare i requisiti di conformità normativa.

**Classificazione dei dati**

La classificazione dei dati è il processo di identificazione dei tipi di dati che un'azienda ha scoperto e quindi l'assegnazione di tag a tali dati per organizzarli in categorie in base al tipo di file, al contenuto e ad altri metadati.

Il processo di classificazione dei dati rende più facile individuare e recuperare i dati sensibili, nonché eliminare le molteplici duplicazioni di dati. Ciò aiuta a ridurre i costi di archiviazione e di backup, aumenta la visibilità su dove risiedono i dati e consente alle aziende di classificare i dati in base al tipo di regolamentazione cui sono soggetti, semplificando il raggiungimento degli obiettivi di conformità.

La scoperta e la classificazione dei dati lavorano insieme per fornire alle aziende una visione completa di quali dati hanno, dove risiedono e quali politiche devono essere adottate per proteggere i dati e garantire la conformità alle normative sulla protezione dei dati. In breve, la scoperta e la classificazione dei dati migliorano notevolmente la protezione dei dati e consentono all'azienda di implementare i controlli necessari per raggiungere la conformità.

**Firewall**

Un firewall è un dispositivo di sicurezza che protegge la tua rete dall'accesso non autorizzato a dati privati. I firewall proteggono anche i computer da software dannoso, creando una barriera tra le reti interne sicure e le reti esterne non attendibili.

I firewall offrono diversi livelli di protezione a seconda delle esigenze di sicurezza del tuo cliente. Per oltre 25 anni, i firewall hanno offerto la prima linea di difesa nei sistemi di sicurezza delle reti. Continua a leggere per scoprire il valore dei firewall nella sicurezza informatica.

**Qual è il ruolo dei firewall nella cybersecurity?**

I firewall sorvegliano i tentativi di traffico indesiderato di accedere al sistema operativo del tuo cliente. Essi formano delle barriere tra i computer e altre reti.

I firewall fungono anche da controllori del traffico, gestendo e convalidando l'accesso alla rete del tuo cliente. La maggior parte dei sistemi operativi e del software di sicurezza ha un firewall preinstallato. Con i firewall, i fornitori di servizi gestiti (MSP) possono eliminare l'incertezza dalla protezione a livello di host. I firewall con un sistema di prevenzione delle intrusioni integrato bloccheranno il malware e gli attacchi a livello di applicazione. Inoltre, reagiscono rapidamente e senza soluzione di continuità per rilevare gli attacchi in tutta la rete.

I firewall di sicurezza delle reti sono preziosi nella gestione del traffico web in quanto riducono al minimo la diffusione delle minacce web.

**Come funziona un firewall?**

I firewall solitamente accolgono le connessioni in ingresso che sono autorizzate ad accedere a una rete. I sistemi di sicurezza consentono o bloccano i pacchetti di dati in base alle regole di sicurezza esistenti. I firewall costruiscono dei punti di controllo che filtrano il traffico web. Questi sistemi ti consentono di esaminare e intervenire sul traffico di rete non autorizzato prima che la rete attaccata subis

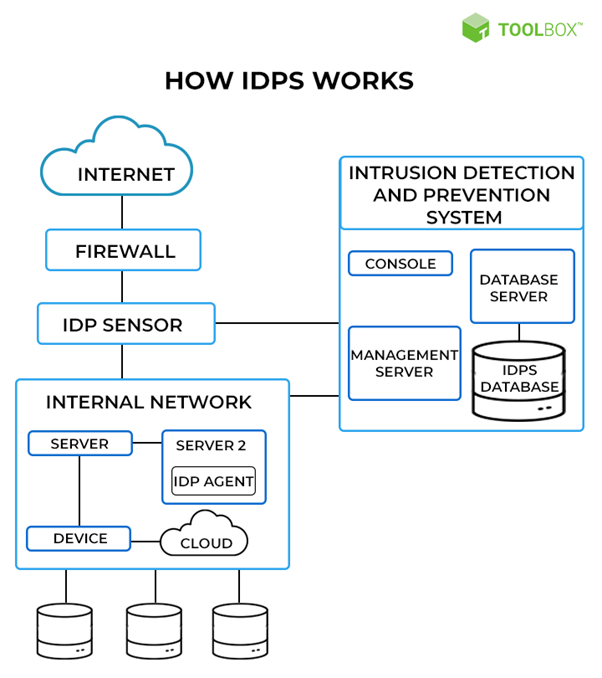
## 

## Intrusion Detection & Prevention Systems

## 

## (IDPS)

Un sistema di rilevamento e prevenzione delle intrusioni (IDPS) monitora una rete alla ricerca di possibili minacce al fine di avvisare l'amministratore e prevenire potenziali attacchi.

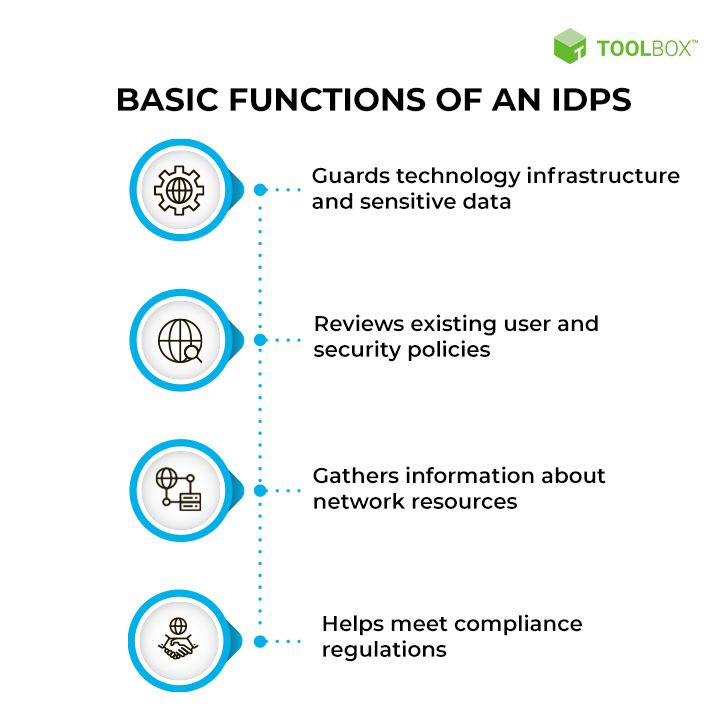


[www.spicework.com](http://www.spicework.com)

Un sistema di rilevamento e prevenzione delle intrusioni è simile al controllo bagagli e sicurezza negli aeroporti. È richiesto un biglietto o una carta d'imbarco per entrare in aeroporto e, una volta all'interno, ai passeggeri non è permesso salire a bordo dei voli fino a quando non sono stati effettuati i necessari controlli di sicurezza. In modo simile, un sistema di rilevamento delle intrusioni (IDS) monitora e segnala solo il traffico dannoso o le violazioni delle politiche. È il predecessore del sistema di prevenzione delle intrusioni (IPS), noto anche come sistema di rilevamento e prevenzione delle intrusioni. Oltre al monitoraggio e alla segnalazione, l'IPS lavora anche per prevenire possibili incidenti con azioni automatizzate.

**Funzioni di base di un IDPS**

Un sistema di rilevamento e prevenzione delle intrusioni offre le seguenti funzionalità:



## Funzioni Base di un IDPS

## 

## Security Information and Event Management

## 

## (SIEM)

SIEM è una soluzione di sicurezza che aiuta le organizzazioni a riconoscere le potenziali minacce alla sicurezza e le vulnerabilità prima che abbiano la possibilità di interrompere le operazioni aziendali. Essa individua anomalie nel comportamento degli utenti e utilizza l'intelligenza artificiale per automatizzare molti dei processi manuali associati alla rilevazione delle minacce e alla risposta agli incidenti ed è diventata un elemento fondamentale nei moderni centri operativi per la sicurezza (SOC) per casi d'uso di sicurezza e gestione della conformità.

Nel corso degli anni, SIEM è maturato diventando più di uno strumento di gestione dei log che lo ha preceduto. Oggi, SIEM offre avanzate analisi del comportamento degli utenti ed delle entità (UEBA) grazie alla potenza dell'intelligenza artificiale e del machine learning. È un sistema altamente efficiente di orchestrazione dei dati per gestire minacce in continua evoluzione e conformità normativa e reporting.

**Come funziona SIEM?**

Al livello più basilare, tutte le soluzioni SIEM svolgono una certa forma di aggregazione, consolidamento e ordinamento dei dati al fine di identificare minacce e rispettare i requisiti di conformità dei dati. Mentre alcune soluzioni possono variare nelle capacità, la maggior parte offre lo stesso insieme di funzionalità di base:

**Gestione dei log**

SIEM cattura dati di eventi da una vasta gamma di fonti in tutta la rete di un'organizzazione. I log e i dati di flusso da utenti, applicazioni, risorse, ambienti cloud e reti vengono raccolti, archiviati e analizzati in tempo reale, dando alle squadre IT e di sicurezza la capacità di gestire automaticamente i log degli eventi della rete e i dati di flusso di rete in un'unica posizione centralizzata.

Alcune soluzioni SIEM si integrano anche con feed di intelligence sulle minacce di terze parti al fine di correlare i propri dati di sicurezza interni con firme e profili di minacce precedentemente riconosciute. L'integrazione con feed di minacce in tempo reale consente alle squadre di bloccare o rilevare nuovi tipi di firme di attacco.[11]

**Correlazione ed analisi degli eventi**

La correlazione degli eventi è una parte essenziale di qualsiasi soluzione SIEM. Utilizzando analisi avanzate per identificare e comprendere intricate strutture di dati, la correlazione degli eventi fornisce informazioni per individuare e mitigare rapidamente le potenziali minacce alla sicurezza aziendale. Le soluzioni SIEM migliorano significativamente il tempo medio di rilevamento (MTTD) e il tempo medio di risposta (MTTR) per le squadre di sicurezza IT scaricando i flussi di lavoro manuali associati all'analisi approfondita degli eventi di sicurezza.[11, 18]

**Monitoraggio degli incidenti e allarmi di sicurezza**

Poiché consentono la gestione centralizzata dell'infrastruttura on-premises e basata su cloud, le soluzioni SIEM sono in grado di identificare tutte le entità dell'ambiente IT. Ciò consente alla tecnologia SIEM di monitorare gli incidenti di sicurezza in tutti gli utenti, dispositivi e applicazioni connessi, classificando nel frattempo i comportamenti anomali man mano che vengono rilevati nella rete. Utilizzando regole di correlazione predefinite e personalizzabili, gli amministratori possono essere avvisati immediatamente e intraprendere azioni appropriate per mitigare il problema prima che si trasformi in problemi di sicurezza più significativi.[11, 19]

**Gestione della conformità e reporting**

Le soluzioni SIEM sono una scelta diffusa per le organizzazioni soggette a diverse forme di conformità normativa. Grazie alla raccolta e all'analisi automatica dei dati che fornisce, SIEM è uno strumento prezioso per la raccolta e la verifica dei dati di conformità in tutta l'infrastruttura aziendale. Le soluzioni SIEM possono generare report di conformità in tempo reale per standard come PCI-DSS, GDPR, HIPPA, SOX e altri standard di conformità, riducendo il peso della gestione della sicurezza e rilevando le potenziali violazioni in anticipo in modo che possano essere affrontate. Molte delle soluzioni SIEM sono dotate di componenti aggiuntivi preconfigurati che consentono di generare report automatici progettati per soddisfare i requisiti di conformità.

## Data Loss Prevention (DLP)

Data Loss Prevention (DLP) è un insieme di strumenti e processi utilizzati per garantire che i dati sensibili non vengano persi, utilizzati in modo improprio o accessibili da utenti non autorizzati.

**Cos'è il Software Data Loss Prevention (DLP)?**

Il software DLP classifica dati regolamentati, confidenziali e critici per l'attività aziendale e individua violazioni delle politiche definite dalle organizzazioni o all'interno di un pacchetto di politiche predefinite, di solito basate su requisiti di conformità normativa come HIPAA, PCI-DSS o GDPR.

Una volta individuate tali violazioni, il DLP impone misure correttive con avvisi, crittografia e altre azioni di protezione per evitare che gli utenti finali condividano accidentalmente o malevolmente dati che potrebbero creare rischi organizzativi.

Il software e gli strumenti di Data Loss Prevention monitorano e controllano le attività degli endpoint, filtrano i flussi di dati sulle reti aziendali e monitorano i dati in cloud per proteggere i dati a riposo, in movimento e in uso. Il DLP fornisce inoltre reporting per soddisfare i requisiti di conformità e audit e identificare aree di debolezza e anomalie per l'analisi forense e la risposta agli incidenti.

**Hai bisogno del Data Loss Prevention? 3 casi d'uso principali per il DLP**

La prevenzione della perdita di dati risolve tre obiettivi principali che sono punti critici comuni per molte organizzazioni: protezione delle informazioni personali / conformità, protezione della proprietà intellettuale (PI) e visibilità dei dati.

Protezione delle informazioni personali / conformità: La tua organizzazione raccoglie e conserva informazioni personali identificabili (PII), informazioni sanitarie protette (PHI) o informazioni di carte di pagamento (PCI)? In tal caso, è molto probabile che tu sia soggetto a normative di conformità, come l'HIPAA (per l'PHI) e il GDPR (per i dati personali dei residenti dell'UE), che richiedono di proteggere i dati sensibili dei clienti. Il DLP può identificare, classificare e contrassegnare dati sensibili e monitorare le attività ed eventi correlati a tali dati. Inoltre, le capacità di reporting forniscono i dettagli necessari per gli audit di conformità.

Protezione della proprietà intellettuale (PI): La tua organizzazione possiede importanti proprietà intellettuale e segreti commerciali o di stato che potrebbero mettere a rischio la salute finanziaria e l'immagine del marchio se fossero persi o rubati? Soluzioni DLP come Digital Guardian che utilizzano la classificazione basata sul contesto possono classificare la proprietà intellettuale in forme strutturate e non strutturate. Con politiche e controlli adeguati, è possibile proteggersi contro l'esfiltrazione indesiderata di tali dati.

Visibilità dei dati: La tua organizzazione cerca di ottenere una maggiore visibilità sul movimento dei dati? Una soluzione DLP aziendale completa può aiutarti a vedere e tracciare i tuoi dati su endpoint, reti e cloud. Ciò ti fornirà una visibilità su come gli utenti individuali all'interno della tua organizzazione interagiscono con i dati.

**Data-Centric Audit and Protection (DCAP)**

Il Data-Centric Audit and Protection (DCAP) è un termine utilizzato da Gartner, una società di ricerca e consulenza aziendale, per descrivere un tipo di sicurezza centrata sui dati. L'obiettivo del DCAP è proteggere la privacy dei dati di un'organizzazione e applicarla a singoli pezzi di dati, non a tutta l'organizzazione.

**Il DCAP si concentra su:**

* Classificazione dei dati
* Conservazione dei dati sensibili
* Governance della sicurezza dei dati
* Protezione dei dati contro l'accesso non autorizzato
* Monitoraggio e audit dei dati

**Come funzionano i Data-Centric Audit & Protection Works**

L'audit e la protezione centrati sui dati riguardano la protezione dei dati, non impediscono agli utenti non autorizzati di hackerare i sistemi. Questo livello di protezione si basa su diverse fasi per garantire la sicurezza dei dati:

**Classificazione dei dati**

Per proteggere i dati sensibili, le organizzazioni aziendali devono sapere dove si trovano le informazioni e quanto sia possibile accedervi. Il primo passo è classificare i dati man mano che vengono creati. Esistono tecnologie di scoperta del contenuto in grado di classificare i dati trovati negli asset dell'organizzazione. I dati sensibili devono essere classificati in modo da poter essere protetti. Ad esempio, i diritti di accesso ai dati vengono assegnati in base a uno schema comune e a politiche.

**Archiviazione di dati sensibili**

Gli strumenti di gestione dei diritti digitali contribuiscono a proteggere i dati sensibili con controlli di accesso e crittografia.

La gestione delle identità e degli accessi (IAM) mantiene i dati sensibili disponibili solo per gli utenti autorizzati.

La crittografia persistente rimarrà con i dati in archiviazione e durante la condivisione ed è il metodo più sicuro. Altrettanto importante quanto la crittografia dei dati in archiviazione e durante la trasmissione è assicurarsi che gli utenti autorizzati dispongano delle giuste chiavi di crittografia. Ciò dovrebbe andare di pari passo con i controlli di accesso.

**Governance della sicurezza dei dati**

Le politiche di governance dei dati definiscono cos'è un dato sensibile, chi ha accesso autorizzato e come possono gestirlo. La governance dei dati deve proteggere i dati e consentire agli utenti di lavorare con essi.

**Monitoraggio e audit dei dati**

L'audit e la protezione centrati sui dati mirano a mantenere i dati sicuri mentre vengono utilizzati. Per garantire questa sicurezza, è possibile utilizzare tecnologie di monitoraggio per proteggerli. Questo comporta l'uso di monitoraggio dell'attività, gestione degli accessi, controllo logico e tecnologie di sicurezza delle applicazioni.

**Protezione dei dati contro l'accesso non autorizzato**

La sicurezza dei dati è l'obiettivo principale del DCAP. È possibile creare processi così sicuri da ostacolare la possibilità di utilizzare effettivamente i dati aziendali. La sicurezza centrata sui dati deve essere bilanciata con la produttività. In caso contrario, le organizzazioni rischiano di perdere i vantaggi derivanti dalla leva dei big data, oppure gli utenti porteranno i dati al di fuori dell'ambiente sicuro, mettendo i dati a rischio.

I dati aziendali sono più preziosi quando vengono condivisi, sia all'interno che all'esterno dell'organizzazione aziendale. Ciò significa anche che i dati possono finire al di fuori del controllo dell'organizzazione. La crittografia può anche contribuire a proteggere i dati sensibili dall'accesso non autorizzato al di fuori del controllo dell'organizzazione.

**Vantaggi dell'audit e della protezione centrati sui dati**

L'audit e la protezione centrati sui dati sono progettati per proteggere i dati aziendali senza ostacolare l'utilizzo dei dati all'interno dell'organizzazione. Una buona sicurezza centrata sui dati può aiutare:

- Consentire alle imprese di utilizzare in modo sicuro servizi IT e fornitori.

- Ridurre il rischio di violazioni dei dati.

- Conformarsi alle direttive normative.

- Gestire i dati, dove sono archiviati, quando sono condivisi e come sono protetti.

- Valutare i rischi dei dati e assegnare priorità agli investimenti nella protezione dei dati.

**Linee guida migliori per l'audit e la protezione centrati sui dati**

La sicurezza centrata sui dati è una strategia olistica. Non discrimina in base al dispositivo, alla tecnologia di archiviazione o alla piattaforma. Assicurati di avere un audit e una protezione centrati sui dati completi con le migliori pratiche come:

- Infrastruttura sicura.

- Reporting e audit.

- Gestione delle chiavi di crittografia.

- Scoperta dei dati.

- Ricerca e cancellazione.

I dati aziendali non sono destinati a durare per sempre. Assicurati che i file temporanei non possano essere ripristinati quando non sono più necessari utilizzando metodi come il crypto-shredding, la cancellazione sicura e la distruzione fisica dei dispositivi e dello storage su disco. La tecnologia di scoperta del

## Application Security

## 

## Code Review

La revisione del codice sicuro è un processo manuale o automatizzato che esamina il codice sorgente di un'applicazione. L'obiettivo di questa revisione è identificare eventuali difetti o vulnerabilità di sicurezza esistenti. La revisione del codice cerca specificamente errori di logica, esamina l'implementazione delle specifiche e verifica le linee guida sullo stile, tra altre attività.

La revisione automatizzata del codice è un processo in cui uno strumento esamina automaticamente il codice sorgente di un'applicazione, utilizzando un insieme predefinito di regole per individuare codice di scarsa qualità. La revisione automatizzata può individuare i problemi nel codice sorgente più rapidamente rispetto all'individuazione manuale.

La revisione manuale del codice coinvolge un essere umano che esamina il codice sorgente, riga per riga, per individuare vulnerabilità. La revisione manuale aiuta a chiarire il contesto delle decisioni di codifica.

**Come funziona il processo di revisione del codice?**

La revisione del codice, che sia manuale, automatizzata o una combinazione delle due, può essere avviata tramite una notifica automatizzata o da un essere umano. Le attuali migliori pratiche per eseguire una revisione del codice solida e sicura coinvolgono l'utilizzo di revisioni manuali e automatiche in combinazione. Questo approccio tandem cattura il maggior numero di possibili problemi.

La revisione del codice sicuro può avvenire in qualsiasi momento durante il ciclo di sviluppo del software (SDLC), ma è più efficace quando viene eseguita in una fase precoce, perché è più facile e veloce apportare correzioni al codice. In particolare, l'uso della revisione automatizzata del codice quando gli sviluppatori stanno effettivamente scrivendo il codice consente di apportare modifiche immediate se necessario. La revisione manuale del codice è molto utile quando viene eseguita durante la fase di commit o quando viene presentata una richiesta di merge al repository. Inoltre, è un modo per rivedere il codice tenendo conto della logica aziendale e delle intenzioni dello sviluppatore.

La revisione automatica consente di analizzare rapidamente e in modo efficiente grandi codebase. Gli sviluppatori eseguono questa revisione utilizzando strumenti open source o commerciali mentre stanno scrivendo il codice, per individuare vulnerabilità in tempo reale. I team di sviluppo più avanzati includono anche strumenti SAST, che possono fornire contributi aggiuntivi, aiutare a individuare vulnerabilità e consentire agli sviluppatori di correggerle prima che il codice venga verificato. I processi di sviluppo più efficaci coinvolgono anche gli sviluppatori che eseguono le proprie autoverifiche mentre scrivono il codice.

La revisione manuale comporta una revisione approfondita dell'intera codebase da parte di uno sviluppatore esperto o senior. Questo processo può essere estremamente noioso e richiedere molto tempo, ma individua difetti, come problemi di logica aziendale, che gli strumenti automatizzati potrebbero non rilevare. L'aggiunta di test di QA può essere utile, ma ci sono comunque scenari che la revisione manuale potrebbe non individuare. La migliore pratica è una combinazione di revisione automatica e manuale.

**Perché è importante la revisione del codice sicuro?**

La revisione del codice sicuro è un processo critico utilizzato dai team di sviluppo più efficienti. Può:

- Ridurre il numero di difetti di consegna riscontrati in una fase successiva del SDLC.

- Ridurre il tempo che gli sviluppatori spendono per correggere difetti in una fase avanzata, aumentando così la produttività.

- Ridurre il numero di bug e vulnerabilità di sicurezza che entrano in produzione.

- Migliorare la coerenza tra le codebase e aumentare la manutenibilità.

- Migliorare la collaborazione, la condivisione delle conoscenze e la produttività degli sviluppatori. Le lezioni apprese possono contribuire a informare lo sviluppo futuro del codice.

- Migliorare il ROI aiutando a rendere i processi più veloci e sicuri, utilizzando meno risorse e tempo.

**Firma del Codice**

La firma del codice è un metodo crittografico utilizzato dagli sviluppatori per dimostrare che un pezzo di software è autentico. Firmando digitalmente app, software o firmware incorporato con una chiave privata, si fornisce agli utenti finali la prova che il codice proviene da una fonte fidata e legittima e che non è stato manomesso da quando è stato pubblicato.

**Perché la Sicurezza della Firma del Codice è Importante**

La firma del codice è un aspetto fondamentale per garantire la sicurezza dei software, ma è altrettanto importante assicurarsi che le chiavi private utilizzate per la firma del codice siano protette in modo adeguato. Ecco alcune ragioni per cui la sicurezza della firma del codice è cruciale:

**Furto delle Chiavi**

Se le chiavi private collegate ai tuoi certificati di firma del codice vengono compromesse, si tratta di un grave problema. Le chiavi di firma del codice rubate sono un obiettivo ambito per gli hacker, che possono venderle o usarle per creare malware firmato che sembra essere stato pubblicato dai tuoi sviluppatori.

**Violazione della Firma**

Gli hacker non hanno bisogno delle tue chiavi per firmare il malware. Se i server di compilazione o le workstation degli sviluppatori con accesso illimitato ai sistemi di firma del codice vengono violati, un attaccante può semplicemente inviare del malware da firmare e distribuire senza essere rilevato.

**Abuso Interno**

Gli sviluppatori si concentrano sul codice, non sulla sicurezza. Le chiavi e i certificati di firma del codice possono essere facilmente abusati o smarriti dagli sviluppatori, rendendo molto più semplice per potenziali attaccanti compromettere l'integrità delle operazioni di firma del codice.

**Sandboxing (Ambienti Isolati)**

Il "sandboxing" è una pratica di sicurezza in cui si utilizza un ambiente isolato, o un "sandbox", per scopi di testing. All'interno del sandbox, è possibile eseguire il codice e analizzarlo in un ambiente sicuro e isolato senza influire sull'applicazione, il sistema o la piattaforma sottostante.

Il sandboxing è particolarmente efficace nel difendersi dalle minacce zero-day, ovvero minacce che non sono state viste in precedenza e non corrispondono a malware noti. Anche se i filtri delle email regolari possono scansionare le email per individuare mittenti maliziosi, tipi di file e URL, le minacce zero-day possono sfuggire a tali filtri tradizionali.

Il sandboxing fornisce un livello di protezione superiore, in particolare quando una email maliziosa supera i filtri del provider. Quando il sandboxing viene utilizzato per il testing, crea un luogo sicuro per installare ed eseguire un programma, in particolare se sospetto, senza esporre il resto del sistema. Se l'applicazione contiene codice dannoso, può essere eseguita all'interno del sandbox senza influenzare gli altri componenti della rete.

**Vantaggi del Sandboxing**

Il sandboxing presenta diversi vantaggi che possono migliorare la sicurezza della tua rete, nonché offrire nuove opzioni per raggiungere gli obiettivi aziendali, sia in ambito IT che in altri settori:

**1. Creazione e Distribuzione di Ambienti:** L'uso di sandbox facilita la creazione e la distribuzione di ambienti su larga scala. Un sandbox ti offre la flessibilità di testare diverse versioni e nuove linee di codice.

**2. Accesso a Funzionalità Avanzate di Rete e Supporto:** Con il giusto tipo di architettura di sandbox, puoi utilizzare funzionalità di rete avanzate e testarle per valutare come possano integrarsi o migliorare il tuo sistema attuale.

**3. Miglioramento della Collaborazione:** Con un ambiente di sandbox, puoi distribuire un'applicazione e concedere l'accesso a persone provenienti da diverse aree aziendali. Possono quindi utilizzare il sandbox e "giocare" con l'applicazione, fornendo feedback al team IT, alla direzione o agli interessati di altri dipartimenti. Se alle squadre è permesso utilizzare un'applicazione e prendere note sulle loro esperienze per un periodo prolungato, i loro risultati possono essere utilizzati per informare meglio la prossima iterazione.

**4. Risparmio di Denaro Aziendale:** Invece di procurare, acquistare, fornire personale e mantenere i propri laboratori di sviluppo interni, è possibile utilizzare sandbox basati su cloud. I soldi che avresti speso per l'acquisizione, l'esecuzione e la manutenzione delle attrezzature possono essere investiti in altri progetti a supporto degli obiettivi aziendali.

**5. Preparazione per gli Attacchi Futuri:** Quando una minaccia è contenuta all'interno dell'ambiente di sandbox, viene isolata e resa disponibile per uno studio da parte del team IT aziendale o da esperti esterni di cibersicurezza. Uno studio attento della minaccia può rivelare schemi che possono essere utilizzati per identificare e prevenire futuri attacchi. È inoltre possibile utilizzare le conoscenze acquisite dalla dissezione della minaccia per identificare vulnerabilità nella rete.

**Web Application Firewall (WAF)**

Un Web Application Firewall (WAF) protegge le applicazioni web da una varietà di attacchi a livello di applicazione, come cross-site scripting (XSS), injection SQL, e avvelenamento dei cookie, tra gli altri. Gli attacchi alle app sono la principale causa di violazioni della sicurezza, poiché rappresentano la porta d'accesso ai tuoi preziosi dati. Con il giusto WAF in atto, puoi bloccare una serie di attacchi mirati a sottrarre tali dati compromettendo i tuoi sistemi.

**Come Funziona un Web Application Firewall (WAF)**

Un WAF protegge le tue app web filtrando, monitorando e bloccando qualsiasi traffico HTTP/S malevolo diretto all'applicazione web e impedisce a dati non autorizzati di lasciare l'app. Lo fa seguendo un insieme di politiche che aiutano a determinare quale traffico sia dannoso e quale sia sicuro. Proprio come un server proxy agisce come intermediario per proteggere l'identità di un client, un WAF funziona in modo simile ma al contrario, in modalità reverse proxy, agendo come intermediario che protegge il server dell'applicazione web da un client potenzialmente dannoso.

I WAF possono essere sotto forma di software, di appliance o forniti come servizio. Le politiche possono essere personalizzate per soddisfare le esigenze uniche della tua applicazione web o di un insieme di applicazioni web. Anche se molti WAF richiedono di aggiornare regolarmente le politiche per affrontare nuove vulnerabilità, i progressi nel machine learning consentono a alcuni WAF di aggiornarsi automaticamente.

**Runtime Application Self-Protection (RASP)**

Runtime Application Self-Protection (RASP) è una soluzione di sicurezza progettata per fornire protezione personalizzata alle applicazioni. Sfrutta la conoscenza dei dati interni e dello stato di un'applicazione per identificare minacce in fase di esecuzione che potrebbero essere state trascurate da altre soluzioni di sicurezza.

**Come funziona RASP**

RASP (Runtime Application Self-Protection) si avvolge attorno e protegge una specifica applicazione, piuttosto che una soluzione di difesa generale a livello di rete o endpoint. Questa posizione di distribuzione più mirata consente a RASP di monitorare gli input, gli output e lo stato interno dell'applicazione che sta proteggendo. Deployando RASP, gli sviluppatori possono identificare le vulnerabilità all'interno delle loro applicazioni. Inoltre, la soluzione RASP può bloccare i tentativi di sfruttare le vulnerabilità esistenti nelle applicazioni in uso.

Il monitoraggio mirato di RASP gli consente di rilevare una vasta gamma di minacce, compresi gli attacchi zero-day. Poiché RASP ha conoscenza dell'interno di un'applicazione, può rilevare cambiamenti comportamentali che potrebbero essere causati da un attacco innovativo. Ciò gli consente di rispondere persino agli attacchi zero-day basati su come influiscono sull'applicazione target.

**Vantaggi di Runtime Application Self-Protection (RASP)**

RASP si differenzia da altre soluzioni di sicurezza informatica per il suo alto livello di focalizzazione su una singola applicazione. Questa focalizzazione gli consente di fornire diversi vantaggi in termini di sicurezza:

**1. Consapevolezza del Contesto:** Quando una soluzione RASP identifica una potenziale minaccia, essa dispone di informazioni contestuali aggiuntive sullo stato attuale dell'applicazione e su quali dati e codice sono interessati. Questo contesto può essere prezioso per investigare, analizzare e risolvere potenziali vulnerabilità, poiché indica dove si trova la vulnerabilità nel codice e come può essere sfruttata.

**2. Visibilità sugli Attacchi a Livello di Applicazione:** RASP ha una profonda visibilità a livello di applicazione perché è integrato con un'applicazione specifica. Questa visibilità, comprensione e conoscenza a livello di applicazione possono contribuire a rilevare una vasta gamma di attacchi e vulnerabilità potenziali.

**3. Protezione Zero-Day:** Sebbene RASP possa utilizzare firme per identificare attacchi, non è limitato alla rilevazione basata su firme. Identificando e rispondendo a comportamenti anomali all'interno dell'applicazione protetta, RASP può rilevare e bloccare persino attacchi zero-day.

**4. Riduzione dei Falsi Positivi:** RASP ha una profonda conoscenza degli interni di un'applicazione, incluso l'effetto di un potenziale attacco sull'esecuzione dell'applicazione. Ciò aumenta notevolmente la capacità di RASP di differenziare gli attacchi veri (che hanno un vero impatto negativo sulle prestazioni e sulla sicurezza dell'applicazione) dai falsi positivi (come tentativi di injection SQL che non vengono mai inclusi in una query SQL). Questa riduzione dei falsi positivi riduce il carico di lavoro sui team di sicurezza e consente loro di concentrarsi sulle minacce reali.

**5. Riduzione dei Costi di CapEx e OpEx:** RASP è progettato per essere di facile implementazione ma in grado di fare una differenza significativa nella vulnerabilità dell'applicazione e nel tasso di falsi positivi rispetto alla correzione manuale e ai firewall delle applicazioni web (WAF).

**6. Facilità di Manutenzione:** RASP funziona basandosi sulla conoscenza di un'applicazione, non su regole di traffico, apprendimento o liste nere. Le squadre SOC amano questa affidabilità e i CISO apprezzano il risparmio di risorse. Le applicazioni diventano autonome e rimangono protette ovunque vadano.

**7. Deployment Flessibile:** Anche se RASP si basa tipicamente su standard HTML, è facile adattare la sua API per funzionare con diversi standard e architetture delle applicazioni. Ciò consente di proteggere anche le applicazioni non web utilizzando standard come XML e RPC.

**8. Supporto Cloud:** RASP è progettato per integrarsi con l'applicazione che protegge e per essere distribuito come parte dell'applicazione. Ciò consente di implementarlo in qualsiasi luogo in cui le applicazioni protette possono essere eseguite, compreso il cloud.

**9. Supporto DevSecOps:** Le soluzioni RASP sono progettate per essere integrate in un flusso di sviluppo e distribuzione (CI/CD) DevOps continuo. Ciò rende RASP di facile implementazione e supporta le operazioni DevSecOps.

## 

## **Software Composition Analysis (SCA)**

L'analisi della composizione del software (Software Composition Analysis o SCA) fornisce un'analisi approfondita dei pacchetti open source utilizzati da un'applicazione. L'SCA evidenzia vulnerabilità e licenze nelle dipendenze per valutazioni di rischio e conformità e può generare un elenco dei componenti software (Software Bill of Materials o SBOM) di tutte le risorse da condividere con gli stakeholder interni e i clienti esterni.

\*\*L'analisi della composizione del software identifica i rischi nei pacchetti open source\*\*

Gli strumenti SCA identificano tutti i pacchetti open source in un'applicazione e tutte le vulnerabilità conosciute di quei pacchetti. Questa conoscenza può essere utilizzata per notificare agli sviluppatori i problemi nel loro codice in modo da poterli risolvere prima che vengano sfruttati. Un buon processo di analisi della composizione del software guarderà oltre i gestori di pacchetti per esaminare anche l'infrastruttura come codice (IaC) e i manifesti di Kubernetes, estrarre immagini per identificare vulnerabilità in quelle immagini.

Gli strumenti SCA con connessioni ai modelli IaC e la scansione illimitata delle dipendenze assicurano che le vulnerabilità non sfuggano alla rilevazione o rimangano irrisolte.

Gli strumenti di analisi della composizione del software possono anche essere utilizzati per generare un elenco dei componenti software (SBOM o software BOM) che include tutti i componenti open source utilizzati da un'applicazione. L'SBOM elenca i dettagli sulla versione del pacchetto e le vulnerabilità conosciute e le licenze per ciascun componente in uso. Ad esempio, per Python, l'elenco includerà tutti i pacchetti nelle dichiarazioni di importazione, come httplib2, insieme al numero di versione, alle vulnerabilità scoperte e alle licenze per ciascun pacchetto.

I programmi SCA dovrebbero consentire la collaborazione tra gli stakeholder, come team di ingegneria, DevOps, sicurezza e conformità. Molte organizzazioni utilizzeranno questi programmi per creare avvisi e/o bloccare il codice prima di unire in repository il codice che include componenti open source che violano le direttive di conformità dell'organizzazione per il controllo dell'esposizione. La determinazione del livello di gravità accettabile per le vulnerabilità e i tipi di licenze dovrebbe coinvolgere gli stakeholder rilevanti.

## Static Application Security Testing (SAST)

Static Application Security Testing (SAST), o analisi statica, è una metodologia di testing che analizza il codice sorgente per individuare vulnerabilità di sicurezza che rendono le applicazioni dell'organizzazione suscettibili a attacchi. Il SAST esegue una scansione dell'applicazione prima che il codice venga compilato. È noto anche come testing "white box".

**Quali problemi risolve il SAST?**

Il SAST si svolge molto presto nel ciclo di vita dello sviluppo del software (SDLC), in quanto non richiede un'applicazione funzionante e può essere effettuato senza che il codice venga eseguito. Aiuta gli sviluppatori a identificare vulnerabilità nelle fasi iniziali dello sviluppo e a risolvere rapidamente i problemi senza interrompere la compilazione o trasmettere vulnerabilità alla versione finale dell'applicazione.

Gli strumenti SAST forniscono un feedback in tempo reale agli sviluppatori mentre scrivono il codice, aiutandoli a risolvere i problemi prima di passare il codice alla fase successiva del SDLC. Ciò impedisce che le problematiche legate alla sicurezza vengano considerate solo come un'aggiunta successiva. Gli strumenti SAST forniscono anche rappresentazioni grafiche dei problemi individuati, dal codice sorgente al punto di iniezione (sink). Questo aiuta a navigare più facilmente nel codice. Alcuni strumenti indicano la posizione esatta delle vulnerabilità e evidenziano il codice a rischio. Gli strumenti possono anche fornire indicazioni dettagliate su come risolvere i problemi e il punto migliore nel codice in cui farlo, senza richiedere una profonda competenza nel dominio della sicurezza.

**Perché il SAST è un'importante attività di sicurezza?**

Gli sviluppatori superano di gran lunga il personale della sicurezza. Può essere impegnativo per un'organizzazione trovare le risorse per effettuare revisioni del codice anche solo per una frazione delle sue applicazioni. Una delle principali forze degli strumenti SAST è la capacità di analizzare il 100% della base di codice. Inoltre, sono molto più veloci delle revisioni manuali del codice sicuro effettuate dagli esseri umani. Questi strumenti possono analizzare milioni di righe di codice in pochi minuti. Gli strumenti SAST identificano automaticamente vulnerabilità critiche, come buffer overflow, SQL injection, cross-site scripting e altre, con elevata affidabilità. Pertanto, l'integrazione dell'analisi statica nel SDLC può produrre risultati significativi sulla qualità complessiva del codice sviluppato.

## Dynamic Application Security Testing (DAST)

La Static Application Security Testing (SAST) è una metodologia di test di sicurezza delle applicazioni (AppSec) in cui i tester esaminano un'applicazione mentre questa è in esecuzione, ma non hanno conoscenza delle interazioni interne dell'applicazione o del design a livello di sistema, e non hanno accesso o visibilità al programma sorgente. Questo tipo di test, noto come "black box", esamina un'applicazione dall'esterno, osserva il suo stato in esecuzione e le risposte alle simulazioni di attacchi effettuate da uno strumento di testing. Le risposte dell'applicazione a tali simulazioni aiutano a determinare se l'applicazione è vulnerabile e potrebbe essere suscettibile a un vero attacco dannoso.

**Come funziona il DAST?**

Il DAST funziona simulando attacchi automatizzati su un'applicazione, imitando un attaccante malintenzionato. L'obiettivo è trovare esiti o risultati non previsti che potrebbero essere sfruttati dagli attaccanti per compromettere un'applicazione. Poiché gli strumenti DAST non dispongono di informazioni interne sull'applicazione o sul codice sorgente, attaccano l'applicazione esattamente come farebbe un hacker esterno, con la stessa conoscenza limitata e le stesse informazioni sull'applicazione.

**Quali problemi risolve il DAST?**

Le applicazioni guidano l'economia mondiale e le organizzazioni sono sotto una pressione enorme per rimanere al passo con il mondo digitale in continua accelerazione. Le imprese devono continuamente innovare in un ambiente in cui attori minacciosi sofisticati e implacabili sono pronti a sfruttare qualsiasi opportunità per disruptare, minacciare dati critici e causare danni. Per navigare con successo in questo nuovo mondo, è fondamentale sviluppare e attuare un piano per garantire che le loro applicazioni siano sicure.

Il DAST funziona simulando attacchi automatizzati su un'applicazione, imitando un attaccante malintenzionato. L'obiettivo è trovare esiti o risultati non previsti che potrebbero essere sfruttati dagli attaccanti per compromettere un'applicazione. Poiché gli strumenti DAST non dispongono di informazioni interne sull'applicazione o sul codice sorgente, attaccano l'applicazione esattamente come farebbe un attore minaccioso esterno, con la stessa conoscenza limitata e le stesse informazioni sull'applicazione.

**Perché il DAST è vitale per la sicurezza delle applicazioni?**

Poiché sempre più imprese fanno affidamento su applicazioni web e mobili per il successo, le vulnerabilità della sicurezza delle applicazioni sono rapidamente diventate la causa più diffusa di violazioni dei dati. Pertanto, è più importante che mai che le organizzazioni proteggano le proprie applicazioni e il proprio codice.

**Le sfide che le organizzazioni stanno attualmente affrontando includono:**

- Il passaggio al cloud e alle tecnologie per applicazioni cloud-native sta rendendo le applicazioni più complesse.

- I microservizi distribuiti in modo massiccio e le funzioni serverless significano che gli sviluppatori sono concentrati esclusivamente sui propri servizi, e nessuno ha una conoscenza completa dell'intera base di codice.

- Con l'aumentare del numero di applicazioni, la dimensione complessiva del codice software distribuito nel cloud espande la superficie di attacco potenziale.

- Con sempre più organizzazioni concentrate sulla trasformazione digitale, la conoscenza del codice legacy sta diminuendo poiché gli sviluppatori vanno in pensione o cambiano ruolo.

- La diffusione di software di terze parti e open source rende le applicazioni più composite. Di conseguenza, una parte significativa del codice dell'applicazione è sviluppato al di fuori del controllo dell'organizzazione.

Implementare il DAST è essenziale non solo per determinare la postura di sicurezza delle applicazioni in esecuzione in produzione e come interagiranno probabilmente con gli utenti finali, ma è diventato essenziale per tenere il passo con la natura in continua evoluzione delle applicazioni e con la conoscenza degli attaccanti. Un efficace DevSecOps inizia con il feedback prodotto dal DAST e la sua integrazione negli strumenti SecOps e DevOps. Alla fine, il DAST individua le vere vulnerabilità che mettono a rischio un'organizzazione e i suoi utenti finali.

## Interactive Application Security Testing (IAST)

IAST (Interactive Application Security Testing) è una tecnologia che analizza il codice alla ricerca di vulnerabilità di sicurezza mentre l'applicazione è in esecuzione tramite un test automatizzato, un tester umano o qualsiasi attività che "interagisce" con la funzionalità dell'applicazione. Questa tecnologia segnala le vulnerabilità in tempo reale, il che significa che non aggiunge tempo extra alla pipeline CI/CD (Continuous Integration/Continuous Deployment).

IAST funziona all'interno dell'applicazione, il che lo rende diverso sia dall'analisi statica (SAST) che dall'analisi dinamica (DAST). Questo tipo di test non esamina l'intera applicazione o la base di codice, ma solo ciò che è attivato dai test funzionali.

IAST funziona meglio quando viene implementato in un ambiente di QA con test funzionali automatizzati in esecuzione.

**Vantaggi dell'IAST:**

1. Velocità dei risultati: IAST segnala le scoperte in tempo reale per la parte dell'applicazione che viene "attivata".

2. Test delle API: Molti test funzionali delle API sono automatizzati, rendendo l'IAST adatto alle squadre che lavorano su microservizi, ecc.

3. Favorisce il riutilizzo di casi di test esistenti: IAST evita la necessità di ricreare script per i test di sicurezza.

L'IAST è meglio utilizzato in combinazione con altre tecnologie di testing. La maggior parte delle organizzazioni ha bisogno sia di soluzioni di assicurazione della sicurezza che di soluzioni incentrate sugli sviluppatori. Le soluzioni di assicurazione della sicurezza, tra cui l'analisi statica, l'analisi dinamica e l'analisi della composizione del software, forniscono alle squadre di sicurezza, ai dirigenti e ai proprietari delle applicazioni valutazioni complete che supportano le decisioni basate sul rischio. Le soluzioni incentrate sugli sviluppatori, come la scansione IDE dell'analisi statica di Veracode, l'analisi della composizione del software e l'IAST, aiutano gli sviluppatori a individuare e correggere i difetti legati alla sicurezza in modo tempestivo e frequente, aiutandoli a imparare a scrivere codice in modo più sicuro e a ridurre il numero di difetti in fasi avanzate del ciclo di sviluppo.

## Conclusioni

La sicurezza delle applicazioni è diventata estremamente critica poiché le applicazioni guidano l'economia mondiale e le organizzazioni sono sotto una pressione incredibile per rimanere al passo con l'accelerazione del mondo digitale. Le aziende devono continuamente innovare in un ambiente in cui attori minacciosi sofisticati e implacabili sono pronti a sfruttare qualsiasi opportunità per disruptare, minacciare dati critici e causare danni. Per navigare con successo in questo nuovo mondo, è fondamentale sviluppare ed eseguire un piano per garantire che le proprie applicazioni siano sicure. Pertanto, l'applicazione di soluzioni di sicurezza è un componente estremamente critico del mondo sicuro, la cui importanza continuerà ad aumentare di anno in anno.

# 4.3 Secure Network Design

Una VPN (Virtual Private Network), ovvero una rete virtuale privata, è progettata per risolvere il problema della mancanza di crittografia in tutti i dati che viaggiano su Internet. Ciò significa che un potenziale aggressore potrebbe intercettare e modificare i dati mentre scorrono sulla rete. Una VPN fornisce una connessione sicura e privata tra due punti che comunicano su una rete pubblica.

**Come funziona una VPN?**

Una VPN offre una connessione sicura ed crittografata tra due punti. Prima di stabilire la connessione VPN, i due estremi della connessione creano una chiave di crittografia condivisa. Questo può essere fatto fornendo una password all'utente o utilizzando un algoritmo di condivisione delle chiavi.

Una volta condivisa la chiave, essa può essere utilizzata per crittografare tutto il traffico che fluisce sulla connessione VPN. Ad esempio, una macchina client cripterà i dati e li invierà all'altro estremo della VPN. In quel punto, i dati verranno decifrati e inoltrati al loro destino. Quando il server di destinazione invia una risposta, l'intero processo si svolgerà in senso inverso.

**Tipi di VPN**

Le VPN sono progettate per fornire una connessione privata e crittografata tra due punti, ma non specificano quali devono essere questi punti. Ciò rende possibile l'uso delle VPN in diversi contesti:

VPN da sito a sito: Una VPN da sito a sito è progettata per collegare in modo sicuro due siti geograficamente distribuiti. La funzionalità VPN è inclusa nella maggior parte dei dispositivi di sicurezza attuali. Ad esempio, un firewall di nuova generazione (NGFW) posizionato al perimetro di una rete protegge la rete aziendale e funge anche da gateway VPN. Tutto il traffico che fluisce da un sito all'altro passa attraverso questo gateway, che crittografa il traffico inviato al gateway dell'altro sito. Quest'ultimo decifra i dati e li inoltra al loro destino.

VPN di accesso remoto: Una VPN di accesso remoto è progettata per collegare in modo sicuro utenti remoti a una rete aziendale. Ad esempio, quando è emersa la pandemia di COVID-19 nel 2020, molte organizzazioni hanno adottato il lavoro da remoto e hanno configurato VPN di accesso remoto sicure per consentire ai clienti remoti di connettersi alle operazioni aziendali critiche.

VPN come servizio: Una VPN come servizio, o una VPN basata su cloud, è ospitata su un'infrastruttura basata su cloud, in modo che i pacchetti provenienti dal client entrino in Internet da quella infrastruttura cloud invece dell'indirizzo locale del client. Le VPN per i consumatori utilizzano comunemente questo modello, consentendo agli utenti di proteggersi quando si connettono a Internet tramite reti Wi-Fi pubbliche non sicure e offrendo un certo grado di anonimato durante l'accesso a Internet.

**Vantaggi di una VPN**

Le VPN possono offrire agli utenti e alle aziende diversi vantaggi, tra cui:

Connessione sicura: Una connessione crittografata di una VPN impedisce a terze parti di intercettare la connessione senza conoscere le chiavi segrete utilizzate per la crittografia, garantendo la sicurezza dei dati in transito.

Reti distribuite semplificate: Qualsiasi computer accessibile tramite Internet pubblico deve avere un indirizzo IP pubblico, direttamente o tramite Network Address Translation (NAT). Una VPN da sito a sito simula una connessione diretta tra le due reti, consentendo loro di utilizzare indirizzi IP privati per il traffico interno.

Controllo degli accessi: Ogni organizzazione ha sistemi e risorse che dovrebbero essere accessibili solo agli utenti interni. Una VPN offre all'utente remoto o al sito un accesso "interno", in quanto il punto terminale della VPN è all'interno del firewall di rete, consentendo di autorizzare l'accesso a queste risorse solo agli utenti remoti autorizzati, senza renderle pubblicamente accessibili.

**È sicura una VPN?**

Una VPN utilizza la crittografia per garantire la sua sicurezza e privacy. In questo modo, le VPN possono soddisfare i tre criteri della sicurezza delle informazioni:

Confidenzialità: La privacy dei dati è garantita crittografando tutti i dati che fluiscono sulla rete pubblica.

Integrità del messaggio: I codici di autenticazione dei messaggi (MAC) assicurano che eventuali modifiche o errori nei dati trasmessi siano rilevabili. In breve, questo sistema rileva quando un messaggio è stato manomesso o interferito in qualche modo, intenzionalmente o accidentalmente.

Autenticazione: Il processo di autenticazione iniziale e di condivisione delle chiavi dimostra l'identità dei due estremi della connessione VPN, impedendo un uso non autorizzato della VPN.

Se una VPN offre tutte le caratteristiche della "triade CIA", può garantire una connessione sicura e privata ai suoi utenti.

**Limitazioni e rischi di sicurezza delle VPN**

Le VPN, sebbene siano progettate per svolgere un ruolo vitale per le aziende moderne, non rappresentano una soluzione perfetta. Presentano diverse limitazioni che influiscono sulla loro usabilità e sulla sicurezza aziendale, tra cui:

1. Visibilità frammentata: Le VPN sono progettate per fornire connettività sicura da punto a punto, con ogni utente VPN su un proprio collegamento. Ciò rende difficile per il team di sicurezza dell'organizzazione mantenere la visibilità completa necessaria per una rilevazione e una risposta efficace alle minacce.

2. Nessuna sicurezza integrata: Un'organizzazione deve implementare soluzioni di sicurezza aggiuntive dietro la VPN per identificare e bloccare contenuti dannosi e per applicare ulteriori controlli di accesso.

3. Instradamento inefficiente: Le VPN possono essere utilizzate in un modello "hub and spoke" per garantire che tutto il traffico passi attraverso lo stack di sicurezza centralizzato dell'organizzazione per l'ispezione. Con il crescente utilizzo del lavoro remoto e delle applicazioni cloud, questa deviazione potrebbe non essere il percorso ottimale tra il client e l'applicazione cloud o Internet.

4. Scalabilità insufficiente: Come soluzione di sicurezza punto-punto, le VPN non scalano bene. Ad esempio, il numero di connessioni VPN da sito a sito in una rete completamente connessa cresce in modo esponenziale con il numero di siti. Ciò crea un'infrastruttura di rete complessa che è difficile da implementare, monitorare e proteggere.

5. Vulnerabilità degli endpoint: Gli endpoint che hanno accesso legittimo alla VPN possono talvolta essere compromessi tramite phishing e altri attacchi informatici. Poiché l'endpoint ha accesso completo alle risorse della VPN, lo stesso vale per l'attore minaccia che ha compromesso l'endpoint.

Molte organizzazioni necessitano di soluzioni di accesso remoto sicuro, e queste limitazioni delle VPN rendono prioritaria la ricerca di alternative alle VPN. Per saperne di più su come implementare l'accesso remoto sicuro nella vostra rete, contattateci. E non esitate a richiedere una prova gratuita delle soluzioni di sicurezza per il lavoro remoto di Check Point per scoprire come possono contribuire a migliorare la produttività e la sicurezza dei telelavoratori della vostra organizzazione.

## Network Segmentation

La segmentazione di rete è un approccio architetturale che suddivide una rete in più segmenti o sottoreti, ognuno dei quali funge da propria piccola rete. Ciò consente agli amministratori di rete di controllare il flusso del traffico di rete tra le sottoreti in base a politiche granulari. Le organizzazioni utilizzano la segmentazione per migliorare il monitoraggio, aumentare le prestazioni, localizzare problemi tecnici e, soprattutto, potenziare la sicurezza.

Con la segmentazione di rete, il personale di sicurezza di rete ha uno strumento potente per prevenire l'accesso di utenti non autorizzati e proteggere gli indirizzi IP statici, che siano utenti interni curiosi o attaccanti malintenzionati, dall'accesso a risorse preziose, come le informazioni personali dei clienti, i record finanziari aziendali e la proprietà intellettuale altamente confidenziale, le cosiddette "gioie della corona" dell'azienda. A causa dell'aumento delle reti definite dal software (SDN), questi asset si trovano spesso distribuiti in ambienti ibridi e multicloud - cloud pubblici, cloud privati e reti definite dal software (SDN) - che devono essere protetti da attacchi e violazioni dei dati. Per comprendere l'uso della sicurezza di rete della segmentazione, è prima necessario considerare il concetto di fiducia nella sicurezza di rete.

**Casi d'uso**

Le organizzazioni possono utilizzare la segmentazione di rete per una varietà di applicazioni, tra cui:

Rete wireless per ospiti: Utilizzando la segmentazione di rete, un'azienda può offrire un servizio Wi-Fi ai visitatori e ai contractor con un rischio relativamente basso. Quando qualcuno accede con le credenziali degli ospiti, entra in una microsegmentazione che fornisce l'accesso a Internet e nient'altro.

Accesso dei gruppi di utenti: Per proteggersi dalle violazioni interne, molte aziende suddividono i singoli dipartimenti interni in sottoreti separate costituite dai membri del gruppo autorizzati e dalle risorse di cui hanno bisogno per svolgere il loro lavoro. L'accesso tra le sottoreti è rigorosamente controllato. Ad esempio, chiunque del reparto ingegneria che tenta di accedere alla sottorete delle risorse umane scatenerà un avviso e un'indagine.

Sicurezza dei cloud pubblici: I fornitori di servizi cloud sono tipicamente responsabili della sicurezza dell'infrastruttura cloud, ma il cliente è responsabile della sicurezza dei sistemi operativi, delle piattaforme, del controllo degli accessi, dei dati, della proprietà intellettuale, del codice sorgente e dei contenuti destinati ai clienti che di solito si trovano sopra l'infrastruttura. La segmentazione è un metodo efficace per isolare le applicazioni in ambienti cloud pubblici e ibridi.

Conformità PCI DSS: Gli amministratori di rete possono utilizzare la segmentazione per isolare tutte le informazioni sulle carte di credito in una zona di sicurezza, essenzialmente una superficie protetta, e creare regole per consentire solo il traffico minimo e legittimo nella zona, negando automaticamente tutto il resto. Queste zone isolate sono spesso reti definite dal software virtualizzate in cui la conformità PCI DSS e la segmentazione possono essere raggiunte tramite firewall virtuali.[32]

**Controllo degli accessi**

Il controllo degli accessi è un componente fondamentale della sicurezza dei dati che stabilisce chi è autorizzato a accedere e utilizzare le informazioni e le risorse aziendali. Attraverso l'autenticazione e l'autorizzazione, le politiche di controllo degli accessi si assicurano che gli utenti siano chi dichiarano di essere e che abbiano l'accesso appropriato ai dati aziendali.

**Come funziona il controllo degli accessi?**

Il controllo degli accessi identifica gli utenti verificando varie credenziali di accesso, che possono includere nomi utente e password, PIN, scansioni biometriche e token di sicurezza. Molti sistemi di controllo degli accessi includono anche l'autenticazione multifattore (MFA), un metodo che richiede più metodi di autenticazione per verificare l'identità di un utente.

Una volta che un utente è autenticato, il controllo degli accessi autorizza il livello appropriato di accesso e le azioni consentite associate alle credenziali dell'utente e all'indirizzo IP.

Esistono quattro principali tipi di controllo degli accessi. Le organizzazioni scelgono tipicamente il metodo che ha più senso in base alle proprie esigenze di sicurezza e conformità uniche. I quattro modelli di controllo degli accessi sono:

Controllo degli accessi discrezionale (DAC): In questo metodo, il proprietario o l'amministratore del sistema protetto, dei dati o delle risorse definisce le politiche per chi è autorizzato ad accedere.

Controllo degli accessi obbligatorio (MAC): In questo modello non discrezionale, le persone ottengono l'accesso in base a un'autorizzazione informazione. Un'autorità centrale regola i diritti di accesso in base a diversi livelli di sicurezza. Questo modello è comune in ambienti governativi e militari.

Controllo degli accessi basato su ruoli (RBAC): RBAC concede l'accesso in base alle funzioni aziendali definite anziché all'identità dell'utente individuale. L'obiettivo è fornire agli utenti l'accesso solo ai dati che sono stati ritenuti necessari per i loro ruoli all'interno dell'organizzazione. Questo metodo ampiamente utilizzato si basa su una complessa combinazione di assegnazioni di ruoli, autorizzazioni e permessi.

Controllo degli accessi basato su attributi (ABAC): In questo metodo dinamico, l'accesso è basato su un insieme di attributi e condizioni ambientali, come l'orario del giorno e la posizione, assegnati sia agli utenti che alle risorse. [37]

**Prevenzione delle perdite di dati (DLP)**

La prevenzione delle perdite di dati (DLP) è una parte della strategia generale di sicurezza di un'azienda che si concentra sulla rilevazione e prevenzione della perdita, della fuoriuscita o dell'abuso dei dati attraverso violazioni, trasmissioni di fuoriuscita e uso non autorizzato.

Una soluzione DLP completa fornisce al team di sicurezza delle informazioni una visibilità completa su tutti i dati presenti in rete, compresi:

Dati in uso: sicurezza dei dati in uso da parte di un'applicazione o di un endpoint attraverso l'autenticazione dell'utente e il controllo degli accessi.

Dati in movimento: garanzia della trasmissione sicura di dati sensibili, confidenziali o proprietari mentre si spostano attraverso la rete tramite crittografia e/o altre misure di sicurezza delle e-mail e della messaggistica.

Dati a riposo: protezione dei dati memorizzati in qualsiasi posizione di rete, compreso il cloud, attraverso restrizioni di accesso e autenticazione dell'utente.

La DLP è anche un modo per le aziende di classificare le informazioni di importanza critica per l'attività e garantire che le politiche aziendali relative ai dati siano conformi alle normative pertinenti, come l'HIPAA, il GDPR e il PCI-DSS. Una soluzione DLP adeguatamente progettata e configurata semplifica la generazione di report per soddisfare questi requisiti di conformità e di audit.

Infine, alcune soluzioni DLP possono anche fornire avvisi, abilitare la crittografia e isolare i dati quando viene rilevata una violazione o un altro incidente di sicurezza. In questo modo, la soluzione DLP può accelerare la risposta agli incidenti identificando aree di vulnerabilità e attività anomala durante il monitoraggio di routine delle reti.

**Ci sono tre tipi di DLP (Prevenzione delle Perdite di Dati):**

**DLP di Rete:** Monitora e protegge tutti i dati in uso, in movimento o inattivi sulla rete aziendale, compreso il cloud.

**DLP di Endpoint:** Monitora tutti gli endpoint, inclusi server, computer, laptop, telefoni cellulari e qualsiasi altro dispositivo su cui i dati vengono utilizzati, spostati o salvati.

**DLP Cloud:** Una sottocategoria del DLP di Rete specificamente progettata per proteggere le organizzazioni che utilizzano repository cloud per lo storage dei dati.

**DLP di Rete:**

Monitora e analizza l'attività di rete e il traffico dell'organizzazione, attraverso una rete tradizionale e il cloud. Questo include il monitoraggio di e-mail, messaggistica e trasferimenti di file, per rilevare quando i dati aziendali critici vengono inviati in violazione delle politiche di sicurezza delle informazioni dell'organizzazione.

Crea un database che registra quando i dati sensibili o confidenziali vengono accessi, chi li ha accessi e, se applicabile, dove i dati si spostano sulla rete.

Fornisce al team di sicurezza delle informazioni una visibilità completa su tutti i dati sulla rete, compresi dati in uso, in movimento o inattivi.

**DLP di Endpoint:**

Monitora tutti gli endpoint di rete, inclusi server, repository cloud, computer, laptop, telefoni cellulari e qualsiasi altro dispositivo su cui i dati vengono utilizzati, spostati o salvati al fine di prevenire perdite, perdite o abusi di dati.

Contribuisce alla classificazione di dati regolamentari, confidenziali, proprietari o critici per l'attività al fine di semplificare i requisiti di reporting e conformità.

Monitora i dati memorizzati sugli endpoint, sia in rete che fuori dalla rete.

**DLP Cloud:**

Scansiona e ispeziona i dati nel cloud per rilevare e crittografare automaticamente le informazioni sensibili prima che vengano ammesse e memorizzate nel cloud.

Mantiene un elenco di applicazioni cloud autorizzate e utenti che possono accedere ai dati sensibili.

Avvisa il team di sicurezza delle informazioni in caso di violazioni delle politiche o attività anomale.

Mantiene un registro degli accessi ai dati basati su cloud e dell'identità dell'utente.

Fornisce una visibilità end-to-end su tutti i dati nel cloud.

**Perché la DLP è importante per le organizzazioni?**

A mano a mano che le aziende si affidano sempre di più a una forza lavoro remota e dispersa e fanno maggiore uso di infrastrutture basate sul cloud, la protezione dei dati sensibili è diventata più complessa. Secondo CrowdStrike Intelligence, le fughe di dati legate al ransomware hanno registrato un aumento dell'82% dal 2020 al 2021. Nel 2021 si sono verificati 2.686 eventi di fughe di dati (rispetto a 1.474 nel 2020) che hanno coinvolto vari settori e industrie, con i settori dell'ingegneria e della produzione che hanno subito le conseguenze più gravi, seguiti dal settore tecnologico.

**Rilevazione di anomalie:**

La rilevazione di anomalie, l'"identificazione di eventi, oggetti o situazioni rare di interesse a causa delle loro caratteristiche diverse dalla maggior parte dei dati elaborati", consente alle organizzazioni di monitorare "errori di sicurezza, difetti strutturali e persino frodi bancarie", secondo DeepAI, e viene descritta in tre forme principali di rilevazione di anomalie: non supervisionata, supervisionata e semi-supervisionata. Gli analisti dei Centri Operativi di Sicurezza (SOC) utilizzano ciascuno di questi approcci con diversi gradi di efficacia nelle applicazioni di sicurezza informatica.

Spesso i fornitori di sicurezza informatica fanno affermazioni audaci sull'intelligenza artificiale (IA) e sul suo ruolo nei loro prodotti di rilevamento di anomalie. Anche se questi fornitori implicano che le loro migliorie di IA possano identificare autonomamente le anomalie, la realtà spesso è diversa. Anche quando questi sistemi possono identificare anomalie (con o senza strumenti di IA), l'identificazione di anomalie è ben lontana dall'essere in grado di neutralizzare le minacce.

L'IA nella sicurezza informatica è diventata uno strumento di marketing. I sistemi che si basano sull'apprendimento automatico o sull'apprendimento supervisionato/non supervisionato possono utilizzare l'IA, ma la tecnologia è datata. L'IA di prima e seconda generazione può essere addestrata per riconoscere anomalie che si discostano da una norma prevista (una base stabilita dagli operatori umani), ma l'IA che apprende in modo autonomo è molto meno comune tra le opzioni disponibili nel mercato della sicurezza informatica. La maggior parte dei sistemi disponibili è limitata dall'interazione umana.

Non c'è dubbio che la rilevazione di anomalie sia utile e necessaria come componente chiave della sicurezza informatica. Strumenti come l'Analisi del Comportamento degli Utenti (UBA) e l'Analisi del Traffico di Rete (NTA) si basano sulla rilevazione di anomalie. La differenza principale tra le soluzioni di sicurezza informatica che utilizzano questi strumenti sta in cosa accade una volta che viene rilevata un'anomalia.

**Sicurezza degli endpoint:**

La sicurezza degli endpoint è la pratica di proteggere i punti finali o i punti di ingresso dei dispositivi degli utenti finali, come desktop, laptop e dispositivi mobili, da essere sfruttati da attori malintenzionati e da campagne di attacchi informatici. I sistemi di sicurezza degli endpoint proteggono questi punti finali su una rete o nel cloud da minacce informatiche. La sicurezza degli endpoint ha evoluto da un tradizionale software antivirus a una protezione completa contro malware sofisticati e minacce "zero-day" in evoluzione.

Le organizzazioni di tutte le dimensioni sono a rischio di attacchi da parte di nazioni, hacktivist, criminalità organizzata e minacce sia maliziose che accidentali da parte di insider. La sicurezza degli endpoint è spesso vista come la prima linea della sicurezza informatica e rappresenta uno dei primi punti in cui le organizzazioni cercano di proteggere le reti aziendali.

Man mano che il volume e la complessità delle minacce informatiche sono cresciuti costantemente, è aumentata la necessità di soluzioni di sicurezza degli endpoint più avanzate. I sistemi di protezione degli endpoint attuali sono progettati per rilevare, analizzare, bloccare e contenere rapidamente gli attacchi in corso. Per fare ciò, devono collaborare tra loro e con altre tecnologie di sicurezza per fornire agli amministratori una visibilità sulle minacce avanzate al fine di velocizzare i tempi di rilevamento e risposta alla rimozione delle minacce.

**Perché la sicurezza degli endpoint è importante:**

Le piattaforme di protezione degli endpoint sono una parte vitale della sicurezza aziendale per diverse ragioni. In primo luogo, nell'attuale mondo aziendale, i dati rappresentano l'attivo più prezioso di un'azienda, e perderli o perdere l'accesso a tali dati potrebbe mettere a rischio l'intera attività fino a rischiare l'insolvenza. Le aziende devono anche fare i conti non solo con un crescente numero di punti finali, ma anche con un aumento del numero di tipi di punti finali. Questi fattori rendono la sicurezza degli endpoint aziendali più difficile da gestire, ma vengono complicati dalle politiche di lavoro remoto e Bring Your Own Device (BYOD), che rendono la sicurezza perimetrale sempre più insufficiente e creano vulnerabilità. Il panorama delle minacce sta diventando più complesso: gli hacker stanno costantemente cercando nuovi modi per ottenere l'accesso, rubare informazioni o manipolare i dipendenti affinché forniscano informazioni sensibili. Aggiungi a ciò l'opportunità, i costi del riposizionamento delle risorse dai obiettivi aziendali al fronteggiamento delle minacce, i costi reputazionali di una violazione su larga scala e i costi finanziari effettivi delle violazioni di conformità, ed è facile capire perché le piattaforme di protezione degli endpoint siano considerate essenziali per la sicurezza delle moderne imprese.

**Come funziona la protezione degli endpoint**

La sicurezza degli endpoint è la pratica di proteggere i dati e i flussi di lavoro associati ai dispositivi individuali che si collegano alla tua rete. Le piattaforme di protezione degli endpoint (EPP) lavorano esaminando i file mentre entrano nella rete. Le moderne EPP sfruttano il potere del cloud per mantenere un database di informazioni sulle minacce in continua crescita, liberando gli endpoint dal sovraccarico associato alla memorizzazione di tutte queste informazioni in locale e dalla manutenzione necessaria per tenerle aggiornate. L'accesso a questi dati nel cloud consente anche una maggiore velocità e scalabilità.

L'EPP fornisce agli amministratori di sistema una console centralizzata, che viene installata su un gateway di rete o un server e consente ai professionisti della sicurezza informatica di controllare la sicurezza per ciascun dispositivo in remoto. Il software client viene quindi assegnato a ciascun endpoint, può essere distribuito come un servizio SaaS e gestito in remoto o installato direttamente sul dispositivo.

Una volta configurato l'endpoint, il software client può inviare aggiornamenti agli endpoint quando necessario, autenticare i tentativi di accesso da ciascun dispositivo e amministrare le politiche aziendali da un'unica posizione. Le EPP proteggono gli endpoint tramite il controllo delle applicazioni, che blocca l'uso di applicazioni non sicure o non autorizzate, e attraverso la crittografia, che aiuta a prevenire la perdita di dati.

Quando l'EPP è configurata, può rilevare rapidamente malware e altre minacce. Alcune soluzioni includono anche un componente di Rilevamento e Risposta degli Endpoint (EDR). Le capacità di EDR consentono la rilevazione di minacce più avanzate, come attacchi polimorfici, malware senza file e attacchi "zero-day". Utilizzando il monitoraggio continuo, la soluzione EDR può offrire una migliore visibilità e una varietà di opzioni di risposta.

Le soluzioni EPP sono disponibili in modelli on-premises o basati su cloud. Mentre i prodotti basati su cloud sono più scalabili e possono integrarsi più facilmente con la tua architettura attuale, alcune normative o regole di conformità possono richiedere sicurezza on-premises.

**Sistemi di prevenzione delle intrusioni**

In breve, un Sistema di Prevenzione delle Intrusioni (IPS), noto anche come Sistema di Rilevamento e Prevenzione delle Intrusioni (IDPS), è una tecnologia che sorveglia una rete per individuare eventuali attività maliziose che tentano di sfruttare una vulnerabilità nota.

La funzione principale di un Sistema di Prevenzione delle Intrusioni è identificare qualsiasi attività sospetta e o rilevarla e consentire (IDS) o prevenirne (IPS) la minaccia. Il tentativo viene registrato e segnalato ai gestori di rete o al personale del Security Operations Center (SOC).

**Perché dovrebbero essere utilizzati i Sistemi di Prevenzione delle Intrusioni (IPS)?**

Le tecnologie IPS possono rilevare o prevenire attacchi alla sicurezza di rete come attacchi di forza bruta, attacchi di Denial of Service (DoS) e sfruttamenti di vulnerabilità. Una vulnerabilità è una debolezza in un sistema software e uno sfruttamento è un attacco che sfrutta quella vulnerabilità per prendere il controllo di un sistema. Quando viene annunciato uno sfruttamento, spesso c'è una finestra di opportunità per gli aggressori per sfruttare quella vulnerabilità prima che venga applicata una patch di sicurezza. In questi casi, un Sistema di Prevenzione delle Intrusioni può essere utilizzato per bloccare rapidamente questi attacchi.

Poiché le tecnologie IPS monitorano il flusso di pacchetti, possono anche essere utilizzate per imporre l'uso di protocolli sicuri e negare l'uso di protocolli non sicuri come le versioni precedenti di SSL o protocolli che utilizzano cifrari deboli.

**Come funzionano i Sistemi di Prevenzione delle Intrusioni (IPS)?**

Le tecnologie IPS hanno accesso ai pacchetti dove sono installate, sia come sistemi di rilevamento delle intrusioni di rete (NIDS) sia come sistemi di rilevamento delle intrusioni dell'host (HIDS). Un NIDS ha una visione più ampia dell'intera rete e può essere implementato in linea nella rete o fuori linea come sensore passivo che riceve pacchetti da una porta di rete TAP o SPAN.

Il metodo di rilevamento impiegato può essere basato su firme o basato su anomalie. Le firme predefinite sono modelli di attacchi di rete ben noti. L'IPS confronta i flussi di pacchetti con la firma per vedere se c'è una corrispondenza di modelli. I sistemi di rilevamento delle intrusioni basati su anomalie utilizzano euristiche per identificare minacce, ad esempio confrontando un campione di traffico con una baseline conosciuta.

**Qual è la differenza tra un Sistema di Rilevamento delle Intrusioni (IDS) e un Sistema di Prevenzione delle Intrusioni (IPS)?**

Nelle prime implementazioni, la tecnologia è stata utilizzata in modalità di rilevamento su appliance di sicurezza dedicate. Man mano che la tecnologia è maturata ed è stata integrata nei dispositivi di Firewall di nuova generazione o UTM, l'azione predefinita è stata impostata per impedire il traffico dannoso.

In alcuni casi, la decisione di rilevare e accettare o prevenire il traffico si basa sulla fiducia nella specifica protezione IPS. Quando c'è una minore fiducia in una protezione IPS specifica, c'è una maggiore probabilità di falsi positivi. Un falso positivo si verifica quando l'IDS identifica un'attività come un attacco, ma l'attività è un comportamento accettabile. Per questo motivo, molte tecnologie IPS hanno anche la capacità di catturare sequenze di pacchetti dall'evento di attacco. Queste sequenze possono quindi essere analizzate per determinare se c'è stata una minaccia reale e per migliorare ulteriormente la protezione IPS.

## Conclusioni

La progettazione di una rete sicura, comprensiva di reti, dati, strumenti e sistemi, con una piattaforma di protezione degli endpoint è una parte vitale della cybersicurezza delle organizzazioni per diverse ragioni. Nel mondo degli affari di oggi, i dati sono l'asset più prezioso di un'azienda o di un'organizzazione, e perdere quei dati o l'accesso a quei dati potrebbe mettere a rischio l'intera organizzazione o azienda fino a rischiare l'insolvenza. Inoltre, le organizzazioni hanno dovuto fare i conti non solo con un crescente numero di implementazioni di reti sicure, ma anche con un aumento del numero di tipi di strumenti e applicazioni più specifici, come gli endpoint.

# 

# 4[.4](https://docs.google.com/document/d/1r9tAENn4JvJzvoSJP-L_gPrG4BwmCnxY/edit#heading=h.7pii0khen2cd) Secure Cloud Controls & Solutions

# 

## Cloud Security Controls

I controlli di sicurezza cloud sono un insieme di misure di sicurezza che proteggono gli ambienti cloud dalle vulnerabilità e mitigano gli effetti di attacchi dannosi.

Un termine ampio, il controllo di sicurezza cloud include tutte le migliori pratiche, procedure e linee guida che devono essere seguite per garantire la sicurezza degli ambienti cloud. Questi controlli di sicurezza cloud aiutano le aziende a affrontare, valutare ed attuare la sicurezza cloud.

Un fornitore di servizi cloud ospita le applicazioni di un'azienda sui suoi server e le rende disponibili via internet nel campo del cloud computing. Allo stesso tempo, il software in loco è distribuito all'interno dei server di un'azienda.

Poiché il cloud computing è diverso dalla distribuzione in loco, è ragionevole aspettarsi che la sicurezza cloud sia altrettanto diversa. Prima di migrare verso il cloud, le organizzazioni devono comprendere come la sicurezza cloud si differenzia dalla sicurezza dei data center. È anche essenziale che le aziende implementino i controlli di sicurezza cloud dopo aver completato la migrazione.

Anche quando le aziende spostano i propri dati sensibili e le applicazioni nel cloud, l'accesso degli utenti avviene in remoto. Di conseguenza, gli amministratori devono anche implementare controlli di accesso basati sul cloud.

**Cosa significa "Controlli di Sicurezza Cloud"?**

Un controllo di sicurezza cloud è una collezione di controlli che consentono all'architettura cloud di proteggersi dalle vulnerabilità e mitigare gli effetti di un attacco dannoso. Si tratta di un termine ampio che comprende tutte le precauzioni, le pratiche e le linee guida che devono essere adottate per proteggere un ambiente di cloud computing.

I controlli di sicurezza cloud aiutano principalmente a considerare, valutare ed attuare la sicurezza nel cloud. La Cloud Security Alliance (CSA) ha creato una Matrice di Controllo Cloud (CCM) progettata per aiutare i potenziali acquirenti di servizi cloud a valutare la sicurezza complessiva di una soluzione cloud.

Sebbene esistano una quantità illimitata di controlli di sicurezza cloud, sono simili ai controlli standard di sicurezza delle informazioni e possono essere categorizzati in diversi domini, tra cui:

- Controlli Deterrenti: Non proteggono l'ambiente cloud ma fungono da avvertimento per un potenziale attaccante.

- Controlli Preventivi: Utilizzati per gestire, rafforzare e proteggere le vulnerabilità all'interno di un cloud.

- Controlli Correttivi: Aiutano a ridurre le conseguenze di un attacco.

- Controlli Detectivi: Usati per identificare o rilevare un attacco.

**Quali tipi di controlli di sicurezza cloud esistono?**

La vostra organizzazione e i fornitori di servizi cloud con cui fate affari condividono la responsabilità di applicare i controlli di sicurezza cloud che proteggono le applicazioni e i dati archiviati o distribuiti nel cloud.

Questi controlli includono misure di sicurezza come l'istituzione di piani di recupero dei dati e di continuità aziendale, la crittografia dei dati e il controllo dell'accesso al cloud per ridurre, mitigare o eliminare vari tipi di rischi.

Sebbene esistano numerosi tipi di audit di sicurezza del cloud computing disponibili, solitamente possono essere classificati nelle quattro categorie elencate di seguito:

**1. Controlli Deterrenti** - I controlli deterrenti sono progettati per tenere lontani gli attori maliziosi da un sistema cloud. Questi controlli informano gli attaccanti che ci saranno conseguenze negative se continuano a rubare dati o ad intraprendere attività sospette. Funzionano più come un sistema di avvertimento. Gli attacchi interni rappresentano un rischio per i fornitori di servizi cloud, quindi un controllo deterrente potrebbe essere che un fornitore di servizi cloud effettui controlli sui precedenti penali dei dipendenti. Questi controlli possono avvisare che chiunque intraprenda un attacco affronterà le conseguenze.

**2. Controlli Preventivi** - I controlli preventivi rafforzano la resilienza del cloud nei confronti degli attacchi eliminando le vulnerabilità di sicurezza. Una misura preventiva potrebbe consistere nella scrittura di codice che disabilita le porte inattive, garantendo che gli hacker non abbiano punti di ingresso adeguati. Un altro modo per ridurre la vulnerabilità agli attacchi è mantenere un sistema di autenticazione dell'utente robusto. I controlli preventivi sono essenziali per rafforzare il sistema. Ad esempio, un'efficace autenticazione dell'utente nel cloud assicura che solo il personale autorizzato possa accedere ai dati.

**3. Controlli Detective** - I controlli detective sono progettati per rilevare e rispondere alle minacce alla sicurezza e agli eventi. Questi controlli detective servono a individuare e rispondere in modo appropriato a qualsiasi evento che potrebbe verificarsi sulla piattaforma online dove si trovano i dati. Tra i controlli detective ci sono software di rilevamento delle intrusioni e strumenti di monitoraggio della sicurezza della rete. Anche il monitoraggio della rete per determinare quando potrebbe verificarsi un attacco è un esempio di controllo detective. In caso di attacco, i controlli detective attivano protocolli di sicurezza e segnalano sia all'attaccante che al proprietario dei dati qualcosa di sospetto. Il monitoraggio della sicurezza del sistema e della rete, i sistemi di rilevamento delle intrusioni e le misure di prevenzione fanno parte dei controlli detective.

**4. Controlli Correttivi** - In caso di violazione della sicurezza, vengono attivati i controlli correttivi. Il compito dei controlli correttivi è limitare i danni causati dall'evento. Un programmatore può scrivere un codice per disconnettere i server dei dati dalla rete quando viene rilevato un tipo specifico di minaccia per prevenire il furto dei dati. I controlli correttivi di solito entrano in gioco durante o dopo l'evento, limitando i danni degli attacchi. Un esempio di ciò è il backup del sistema in caso di attacco.

**Quali sono i controlli di sicurezza cloud applicabili?**

La sicurezza del cloud computing si riferisce in generale a varie politiche, tecnologie e controlli implementati per proteggere i dati del cloud, le applicazioni e l'infrastruttura di cloud computing correlata. L'architettura di sicurezza del cloud è efficace solo quando si dispone di un adeguato sistema e processo di sicurezza e difesa.

Le preoccupazioni sulla sicurezza legate al cloud computing rientrano in due categorie principali:

1. Problemi di sicurezza affrontati dai fornitori di servizi cloud.

2. Problemi di sicurezza affrontati dai clienti che utilizzano software di sicurezza cloud.

La responsabilità di proteggere i dati è suddivisa tra i fornitori di servizi cloud e i clienti. Il fornitore di servizi cloud deve sempre garantire che l'infrastruttura sia sicura e che le informazioni dei propri clienti siano protette.

D'altro canto, gli utenti dovrebbero controllare attentamente le proprie pratiche di sicurezza cloud e attuare protocolli di sicurezza come password robuste e metodi di autenticazione in modo che solo il personale autorizzato possa accedere ai dati.

La disponibilità fisica diminuisce quando un'organizzazione decide di portare i propri dati online con un software o un'applicazione di sicurezza cloud. Pertanto, è necessario tenere sotto controllo i dipendenti che hanno accesso a queste informazioni, poiché gli attacchi interni rappresentano una grande minaccia per le organizzazioni e le aziende. Inoltre, spesso è necessario sorvegliare i data center.

Di seguito sono riportate le utili funzionalità vitali che devono essere affrontate durante l'implementazione dei controlli di sicurezza cloud. Implementando questi controlli, è possibile sfruttare l'agilità e la focalizzazione sul cliente del cloud senza sacrificare la sicurezza o la conformità necessaria:

**Protezione dei dati in ambienti cloud**

Se scegli di ospitare dati sensibili presso un fornitore di servizi cloud, perdi il controllo dell'accesso fisico al server. Questo crea ulteriori vulnerabilità di sicurezza poiché non puoi più avere un ruolo nel determinare chi ha accesso fisico ai server.

Un dipendente del fornitore di servizi cloud può accedere illegalmente, modificare o copiare dati e persino distribuirli ad altri. Per prevenire attacchi interni, i fornitori di servizi cloud devono effettuare dettagliati controlli dei precedenti dei dipendenti e mantenere un accesso rigoroso e trasparente ai server e all'infrastruttura IT.

Inoltre, sapere cosa fanno i tuoi utenti e i tuoi sistemi richiede la revisione dei file di registro. Nel cloud, è probabile che tu debba fare affidamento sul tuo fornitore per fornire i file di registro, e probabilmente non sarai in grado di esaminare i registri dell'infrastruttura condivisa sottostante.

Dovresti assicurarti che i registri vengano aggregati e trasferiti nel tuo strumento di gestione degli eventi nonostante le potenziali limitazioni delle informazioni.

**Visibilità centralizzata dell'infrastruttura cloud**

Una delle sfide più impegnative nella sicurezza del cloud computing è la mancanza di visibilità sulle applicazioni e servizi implementati nel cloud. La mancanza di visibilità significa che non puoi raccogliere efficientemente informazioni sullo stato di sicurezza delle applicazioni e dell'infrastruttura implementate nel cloud.

Questo può essere dovuto al fatto che molti sistemi diversi lavorano insieme nel cloud, o non c'è trasparenza tra l'azienda e il fornitore di servizi cloud.

I fondamenti del controllo di sicurezza del cloud includono la visibilità centralizzata sulle politiche di sicurezza, le impostazioni di configurazione e l'attività dell'utente, nonché i rischi che possono essere archiviati nei repository online. Questo riduce la probabilità che il tuo team di sicurezza trascuri una vulnerabilità nella sicurezza del cloud a causa di una configurazione errata o di una mancanza di attività anomala che potrebbe indicare un attacco.

Il problema è che diversi cloud offrono diverse opzioni di configurazione e i programmatori spesso selezionano queste opzioni senza competenze di sicurezza. Non è facile ottenere visibilità attraverso le istanze e i cloud.

Le squadre di sicurezza necessitano di una visibilità centralizzata sulla loro infrastruttura cloud per ridurre tali rischi. Gli strumenti di protezione del carico di lavoro cloud (CWP), strettamente integrati nei sistemi di gestione e sicurezza del cloud, possono aiutare in questo compito.

Gli strumenti di protezione del carico di lavoro cloud (CWP) consentono alle squadre di sicurezza di monitorare ed valutare lo stato di configurazione dei servizi esistenti e la postura complessiva di sicurezza dell'ambiente cloud. Il monitoraggio automatico della configurazione consente alle squadre IT di identificare rapidamente e rispondere alle configurazioni errate di sicurezza, riducendo il tempo necessario per implementare correzioni e aumentando la sicurezza.

Le capacità critiche degli strumenti di protezione del carico di lavoro e della piattaforma includono:

- Analisi del traffico

- Esame dei dati archiviati nel cloud per contenuti sensibili o maligni

- Monitoraggio e valutazioni regolari delle configurazioni

- Raccomandazioni su come migliorare le aree vulnerabili dell'ambiente cloud

- Avvertenze per problemi di configurazione

- Identificazione di problemi di compatibilità dovuti a configurazioni errate

- Integrazione a livello nativo con sistemi di gestione e sicurezza cloud

Nel caso dei sistemi informatici legacy implementati e gestiti in locale, le organizzazioni IT mantengono il controllo completo su ogni parte dell'infrastruttura IT lungo l'intero stack tecnologico. Delegare parte della tua infrastruttura IT a un fornitore di servizi cloud comporta invece la rinuncia a parte del controllo su come quell'infrastruttura viene implementata, gestita e configurata.

Di conseguenza, le organizzazioni IT devono sempre più fare affidamento sui fornitori di servizi cloud per prendere decisioni amministrative che impongano un alto livello di sicurezza.

A differenza dei tradizionali data center, il cloud computing si basa su un modello di responsabilità condivisa in cui il cliente e altri controllano alcune impostazioni di sicurezza fornite dal fornitore di cloud pubblico.

La visibilità della tua postura di sicurezza attraverso i cloud richiede una stretta coordinazione tra la tua soluzione e l'ambiente cloud sottostante. Ciò significa un'integrazione a livello di API con strumenti come Amazon Inspector e VPC Flow logs e GuardDuty per AWS, Stack Event, Security Center per Azure e Stream Drivers per Google Cloud Platform.

Potrebbe essere necessaria una soluzione di cloud access security broker (CASB) che si integri profondamente con il servizio SaaS per identificare rischi e problemi di configurazione.

**Sicurezza cloud tramite autenticazione dell'utente e gestione degli accessi**

I servizi cloud dovrebbero essere protetti da un nome utente e una password. Tuttavia, un attore malintenzionato rischia sempre di rubare le credenziali di accesso, ottenere un accesso non autorizzato ai servizi cloud e rubare o modificare i dati.

Un aggressore può anche installare codice dannoso nel sistema. I fornitori di servizi cloud devono implementare un sistema di autenticazione sicura e di gestione degli accessi per proteggere i clienti da tali attacchi.

Controllare chi può accedere ai tuoi dati e gestire i loro privilegi è fondamentale per la sicurezza delle informazioni. Per i tuoi dati nel cloud, devi comprendere i controlli del provider cloud sull'accesso dei propri dipendenti ai tuoi sistemi.

Dovresti estendere la tua gestione delle identità e degli accessi al cloud utilizzando la sicurezza federata con accesso singolo e privilegi basati su ruoli per ridurre il numero di identità e privilegi da gestire. I privilegi principali, che dovrebbero sempre essere ridotti al minimo, devono essere gestiti ancora più attentamente nel cloud.

**Protezioni aggiuntive a livello di applicazione web**

Ulteriori vulnerabilità sorgono quando non è chiaro chi è responsabile della protezione dell'infrastruttura cloud. La sicurezza delle applicazioni e dei dati basati su cloud è di competenza della tua azienda. I fornitori di servizi cloud si prendono cura solo dell'infrastruttura.

Per adempiere al meglio al loro ruolo nel modello di responsabilità condivisa, le tue organizzazioni dovrebbero utilizzare firewall per le applicazioni web per proteggere le applicazioni web. La rilevazione delle minacce alle app è diversa quando le app vengono eseguite nel cloud anziché in locale, poiché il controllo dell'accesso a indirizzi IP specifici non funziona con le app implementate nel cloud.

Qui, il rilevamento delle minacce dovrebbe avvenire nel contenuto dell'applicazione, non nel traffico. Ciò richiede costanti aggiustamenti granulari che non puoi gestire manualmente.

Solo un approccio che sfrutta la potenza e la velocità dell'IA sarà in grado di proteggere le applicazioni basate su cloud di oggi. L'apprendimento automatico può aiutare a rilevare il tipo di comportamento dell'utente o dell'applicazione che indica un problema e a implementare protezioni che nessun approccio assistito dall'essere umano può eguagliare in termini di velocità o precisione.

**Minacce da feed di informazioni sulle minacce**

Più complesso è il tuo ambiente cloud, più è vulnerabile alle minacce. La massima sicurezza cloud è fornita da una soluzione completa che raccoglie tutti i servizi cloud della tua azienda in un unico sistema.

Una buona soluzione dovrebbe includere feed di informazioni sulle minacce dinamiche con un'ampia copertura di informazioni sulle minacce globali e locali. Quando selezioni controlli di sicurezza cloud, cerca fornitori le cui soluzioni siano basate su dati raccolti da tutti i sensori che hanno distribuito.

**Automazione della sicurezza cloud**

Il campo della cibersicurezza è insufficiente per soddisfare tutte le esigenze aziendali a causa del gap delle competenze nella cibersicurezza. Oggi, i professionisti della cibersicurezza sono molto richiesti, e le attuali squadre di sicurezza presentano diverse lacune di competenza. In definitiva, tali problematiche espongono le aziende a una vasta gamma di minacce.

Fino a quando l'industria della cibersicurezza non sarà in grado di soddisfare le esigenze delle imprese e le richieste di un pool di talenti più grande e più competente, gli architetti della sicurezza sono incoraggiati ad aiutare le organizzazioni ad automatizzare le loro funzioni di sicurezza ogni volta che possibile.

Un approccio attualmente utilizzato include plugin che forniscono agli amministratori una maggiore visibilità all'interno di ecosistemi multifornitore, automazione e gestione semplificata. Quando avvengono modifiche alle applicazioni, le squadre IT e DevOps possono rimanere aggiornate senza dover aggiornare le politiche di sicurezza ogni volta che cambiano le funzionalità delle applicazioni.

Gli script di configurazione della sicurezza, disponibili per il download dai fornitori di sicurezza, possono anche aiutare ad automatizzare i processi di sicurezza.

**Gestione delle patch nel cloud**

Anche se i tuoi server sono nel cloud, la necessità di conoscere le vulnerabilità dei tuoi sistemi e applicare le patch non scompare. Per alcuni tipi di servizi cloud, il fornitore risolverà questi problemi, ma rimani responsabile per alcune versioni dell'Infrastructure as a Service.

La sfida nel tenere traccia dell'applicazione delle patch diventa più complessa poiché i server nel cloud sono molto più frequentemente attivati e disattivati. Vorrai eseguire scansioni continue per le vulnerabilità di sicurezza, non periodicamente.

Un Cloud Access Security Broker, o CASB, è un software ospitato nel cloud o un software o hardware in loco che funge da intermediario tra gli utenti e i fornitori di servizi cloud. La capacità di un CASB di colmare le lacune nella sicurezza si estende su ambienti di software come servizio (SaaS), piattaforma come servizio (PaaS) e infrastruttura come servizio (IaaS). Oltre a fornire visibilità, un CASB consente anche alle organizzazioni di estendere la portata delle proprie politiche di sicurezza dall'infrastruttura in loco esistente al cloud e di creare nuove politiche per il contesto specifico del cloud. I CASB sono diventati una parte vitale della sicurezza aziendale, consentendo alle aziende di utilizzare in modo sicuro il cloud proteggendo i dati sensibili dell'azienda. Il CASB funge da centro di applicazione delle politiche, consolidando vari tipi di applicazione delle politiche di sicurezza e applicandoli a tutto ciò che l'azienda utilizza nel cloud, indipendentemente dal tipo di dispositivo che cerca di accedervi, inclusi smartphone non gestiti, dispositivi IoT o laptop personali. Con l'incremento della mobilità della forza lavoro, la crescita del BYOD e la presenza dell'uso non autorizzato di servizi cloud da parte dei dipendenti, noto come Shadow IT, la capacità di monitorare e regolamentare l'uso di applicazioni cloud come Microsoft 365 è diventata essenziale per gli obiettivi della sicurezza aziendale. Piuttosto che vietare completamente i servizi cloud e potenzialmente influire sulla produttività dei dipendenti, un CASB consente alle aziende di adottare un approccio dettagliato alla protezione dei dati e all'applicazione delle politiche, consentendo di utilizzare in modo sicuro servizi cloud che risparmiano tempo, migliorano la produttività ed è economicamente vantaggioso.

**Cosa offrono i CASB**

Molte delle funzionalità di sicurezza dei CASB sono uniche rispetto a quelle offerte da altri controlli di sicurezza, come i firewall per le applicazioni enterprise/web e i gateway web sicuri, e possono includere:

* Governance e valutazione del rischio nel cloud
* Prevenzione della perdita di dati
* Controllo sulle funzionalità native dei servizi cloud, come collaborazione e condivisione
* Prevenzione delle minacce, spesso basata sull'analisi del comportamento dell'utente ed dell'entità (User and Entity Behavior Analytics, UEBA)
* Auditing della configurazione
* Rilevamento di malware
* Crittografia dei dati e gestione delle chiavi
* Integrazione SSO e IAM
* Controllo di accesso contestuale

**Come funzionano i CASB?**

Il compito di un broker di sicurezza per l'accesso al cloud (CASB) è fornire visibilità e controllo sui dati e sulle minacce nel cloud per soddisfare i requisiti di sicurezza aziendale. Questo avviene attraverso un processo in tre fasi:

1. Scoperta: La soluzione CASB utilizza la scoperta automatica per compilare un elenco di tutti i servizi cloud di terze parti, nonché di chi li sta utilizzando.

2. Classificazione: Una volta rivelata l'entità completa dell'uso del cloud, il CASB determina il livello di rischio associato a ciascuno di essi stabilendo che tipo di applicazione è, che tipo di dati contiene e come vengono condivisi.

3. Rettifica: Dopo che è noto il rischio relativo di ciascuna applicazione, il CASB può utilizzare queste informazioni per stabilire una politica per i dati dell'organizzazione e l'accesso degli utenti per soddisfare i loro requisiti di sicurezza e intraprendere automaticamente azioni in caso di violazione.

I CASB offrono inoltre ulteriori livelli di protezione mediante prevenzione del malware e crittografia dei dati.

## Conclusioni

Il cloud computing è un settore promettente (relativamente nuovo nell'ambito dell'IT) che fornisce soluzioni efficaci per varie organizzazioni ospitando le loro applicazioni e dati sui suoi server e rendendoli disponibili via Internet. Il cloud computing è ancora un campo in sviluppo che offre diverse opportunità di carriera nel campo dell'IT. Dato che l'hosting dei dati delle organizzazioni avviene sui server, la sicurezza è un argomento critico in cui le implementazioni di sicurezza cloud sono fondamentali, richiedendo una vasta gamma di sforzi per soddisfare i requisiti di sicurezza. Con l'aumento della quantità di dati memorizzati online, il cloud computing svolge un ruolo sempre più importante nel rendere possibile l'utilizzo sicuro di servizi cloud che consentono di risparmiare tempo, aumentare la produttività ed essere più economici.

# L’angolo del Geek

**Data-Centric Audit and Protection (DCAP)**

Data-centric audit and protection (DCAP) è un termine utilizzato da Gartner, una società di ricerca e consulenza aziendale, per descrivere un tipo di sicurezza incentrata sui dati. L'obiettivo di DCAP è proteggere la privacy dei dati di un'organizzazione e applicarla a specifici pezzi di dati, non all'intera organizzazione.

DCAP si concentra su:

- Classificazione dei dati

- Archiviazione dei dati sensibili

- Governance della sicurezza dei dati

- Protezione dei dati dall'accesso non autorizzato

- Monitoraggio e audit dei dati

Leggi di più:

<https://www.microfocus.com/en-us/what-is/data-centric-audit-protection-dcap>

<https://www.lepide.com/blog/what-is-data-centric-audit-and-protection-dcap/>

<https://www.trustradius.com/data-centric-audit-protection>

<https://www.ibm.com/docs/en/hpdc/1.2.3?topic=overview-data-centric-protection>

## Conclusioni

In questa unità, abbiamo brevemente esaminato vari controlli e soluzioni di sicurezza, che sono parametri implementati per proteggere varie forme di dati e infrastrutture importanti per un'organizzazione, che vanno dalle scelte chiave di progettazione, architettura e implementazione fatte dalle organizzazioni per soddisfare requisiti di sicurezza specifici per sistemi o componenti di sistema. Inoltre, è stata affrontata l'area del cloud computing in quanto fornisce servizi unici per ospitare i dati delle organizzazioni su piattaforme cloud, che devono ancora progredire nei servizi e negli aspetti della sicurezza, simili ad altre soluzioni e strumenti di controllo della sicurezza e studi.

## Quiz

**Un'operazione che spesso presenta vulnerabilità di cross-site scripting (XSS) è?**

1. Un utente visita la homepage di un sito.
2. Un sito richiede all'utente il suo nome utente e la password.
3. **Un sito produce un messaggio di errore per un nome utente non valido.**
4. Un utente fa clic su un collegamento ipertestuale per visitare un'altra pagina nello stesso sito.
5. Un utente fa clic su un collegamento ipertestuale per visitare un'altra pagina in un sito diverso.

**2. Una strategia comune per prevenire le vulnerabilità XSS è?**

1. Educare gli utenti a riconoscere le pagine web sicure da quelle non sicure.
2. Eseguire l'escape dell'input dell'utente non appena possibile.
3. **Evitare l'uso di JavaScript nel tuo sito.**
4. Utilizzare un linguaggio di programmazione interpretato come Java o C#.
5. Assicurarsi che il database sia configurato per una forte sicurezza.

**3. In un'applicazione web tipica a più livelli con una DMZ, le pratiche standard di sicurezza indicano che la crittografia è richiesta quando (scegli 1 o più risposte):**

1. Viene visualizzata la pagina di accesso al form.
2. I numeri di carta di credito vengono trasmessi al sito.
3. **I numeri di carta di credito vengono trasmessi tra due macchine all'interno della stessa DMZ.**
4. I numeri di carta di credito vengono trasmessi tra due macchine all'interno della rete sicura dietro la DMZ.
5. Mai. La crittografia è sempre richiesta.

**4. Qual è la principale vulnerabilità che porta alle violazioni dei dati?**

1. **Iniezione SQL**
2. Cross-Site Scripting (XSS)
3. Cross-Site Request Forgery (CSRF)
4. Esposizione di dati sensibili

**Fonti**

1. Aldhyani, T.H.; Alkahtani, H. Attacks to automatous vehicles: A deep learning algorithm for cybersecurity. Sensors 2022, 22, 360. [CrossRef]

2. Alrawi, O.; Lever, C.; Antonakakis, M.; Monrose, F. SoK: Security Evaluation of Home-Based IoT Deployments. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2019; pp. 1362–1380.

3. Al-Saud, M.; Eltamaly, A.M.; Mohamed, M.A.; Kavousi-Fard, A. An intelligent data-driven model to secure intravehicle communications based on machine learning. IEEE Trans. Ind. Electron. 2019, 67, 5112–5119. [CrossRef]

4. Aly, M.; Khomh, F.; Haoues, M.; Quintero, A.; Yacout, S. Enforcing security in Internet of Things frameworks: A Systematic Literature Review. Internet Things 2019, 6, 100050. [CrossRef]

5. Ammar, M.; Russello, G.; Crispo, B. Internet of Things: A survey on the security of IoT frameworks. J. Inf. Secur. Appl. 2018, 38, 8–27. [CrossRef]

6. Apostu, S.; Burkacky, O.; Deichmann, J.; Doll, G. Automotive Software and Electrical/Electronic Architecture: Implications for OEMs. 2019. Available online: https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/automotivesoftware-andelectrical-electronic-architecture-implications-for-oems (accessed on 16 July 2022).

7. Bali, R.S.; Jaafar, F.; Zavarasky, P. Lightweight Authentication for MQTT to Improve the Security of IoT Communication. In Proceedings of the 3rd International Conference on Cryptography, Security and Privacy (ICCSP ’19), Kuala Lumpur, Malaysia, 19–21 January 2019; pp. 6–12.

8. Bandur, V.; Selim, G.; Pantelic, V.; Lawford, M. Making the case for centralized automotive e/e architectures. IEEE Trans. Veh. Technol. 2021, 70, 1230–1245. [CrossRef]

9. Carvajal-Roca, I.E.; Wang, J.; Du, J.; Wei, S. A Semi-Centralized Dynamic Key Management Framework for In-Vehicle Networks. IEEE Trans. Veh. Technol. 2021, 70, 10864–10879. [CrossRef]

10.Cheshire, S.; Krochmal, M. DNS-Based Service Discovery. Available online: https://tools.ietf.org/html/ rfc6763 (accessed on 15 March 2023).

11. Cheshire, S.; M.K. Multicast DNS. Available online: https://tools.ietf.org/html/rfc6762 (accessed on 15 March 2023).

12. D’Angelo, G.; Castiglione, A.; Palmieri, F. A cluster-based multidimensional approach for detecting attacks on connected vehicles. IEEE Internet Things J. 2020, 8, 12518–12527. [CrossRef]

13. Dizdarevi´c, J.; Carpio, F.; Jukan, A.; Masip, X. A Survey of Communication Protocols for Internet of Things and Related Challenges of Fog and Cloud Computing Integration. ACM Comput. Surv. 2019, 51, 116. [CrossRef]

14. Dinculean˘a, D. Vulnerabilities and Limitations of MQTT Protocol Used between IoT Devices. Appl. Sci. 2019, 9, 848. [CrossRef]

15. E. Rescorla, N.M. Datagram Transport Layer Security Version 1.2. Available online: https://tools.ietf.org/ html/rfc6347 (accessed on 15 March 2023).

16. El-Rewini, Z.; Sadatsharan, K.; Selvaraj, D.F.; Plathottam, S.J.; Ranganathan, P. Cybersecurity challenges in vehicular communications. Veh. Commun. 2020, 23, 100214. [CrossRef]

17. Groza, B.; Popa, L.; Murvay, P.S. Highly efficient authentication for CAN by identifier reallocation with ordered CMACs. IEEE Trans. Veh. Technol. 2020, 69, 6129–6140. [CrossRef]

18. Guo, J.; Li, X.; Liu, Z.; Ma, J.; Yang, C.; Zhang, J.; Wu, D. TROVE: A context-awareness trust model for VANETs using reinforcement learning. IEEE Internet Things J. 2020, 7, 6647–6662. [CrossRef]

19. Guan, T.; Han, Y.; Kang, N.; Tang, N.; Chen, X.; Wang, S. An overview of vehicular cybersecurity for intelligent connected vehicles. Sustainability 2022, 14, 5211. [CrossRef]

20. Hanes, D.; Salquiero, G.; Grossetete, P.; Barton, R.; Henry, J. IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things; Cisco Press: Indianapolis, IN, USA, 2017.

21. He, Y.; Jia, Z.; Hu, M.; Cui, C.; Cheng, Y.; Yang, Y. The Hybrid Similar Neighborhood Robust Factorization Machine Model for Can Bus Intrusion Detection in the In-Vehicle Network. IEEE Trans. Intell. Transp. Syst. 2021, 1, 1–9. [CrossRef]

22. Hossain, M.D.; Inoue, H.; Ochiai, H.; Fall, D.; Kadobayashi, Y. LSTM-based intrusion detection system for in-vehicle can bus communications. IEEE Access 2020, 8, 185489–185502. [CrossRef]

23.Karopoulos, G.; Kambourakis, G.; Chatzoglou, E.; Hernández-Ramos, J.L.; Kouliaridis, V. Demystifying In-Vehicle Intrusion Detection Systems: A Survey of Surveys and a Meta-Taxonomy. Electronics 2022, 11, 1072. [CrossRef]

23. Katragadda, S.; Darby, P.J.; Roche, A.; Gottumukkala, R. Detecting low-rate replay-based injection attacks on in-vehicle networks. IEEE Access 2020, 8, 54979–54993. [CrossRef]

24. Lenard, T.; Bolboacă, R.; Genge, B.; Haller, P. MixCAN: Mixed and backward-compatible data authentication scheme for controller area networks. In Proceedings of the 2020 IFIP Networking Conference (Networking), Paris, France, 22–26 June 2020; pp. 395–403.

25.Liu, H.; Spink, T.; Patras, P. Uncovering Security Vulnerabilities in the Belkin WeMo Home Automation Ecosystem. In Proceedings of the 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kyoto, Japan, 11–15 March 2019; pp. 894–899.

26.Li, X.; Hu, Z.; Xu, M.; Wang, Y.; Ma, J. Transfer learning based intrusion detection scheme for Internet of vehicles. Inf. Sci. 2021, 547, 119–135. [CrossRef]

27. Lin, Y.; Chen, C.; Xiao, F.; Avatefipour, O.; Alsubhi, K.; Yunianta, A. An Evolutionary Deep Learning Anomaly Detection Framework for In-Vehicle Networks—CAN Bus. IEEE Trans. Ind. Appl. 2020, 1, 1–14. [CrossRef]

28.Loi, F.; Sivanathan, A.; Gharakheili, H.H.; Radford, A.; Sivaraman, V. Systematically Evaluating Security and Privacy for Consumer IoT Devices. In Proceedings of the Workshop on Internet of Things Security and Privacy (IoTS&P), Dallas, TX, USA, 3 November 2017.

29. Lo, W.; Alqahtani, H.; Thakur, K.; Almadhor, A.; Chander, S.; Kumar, G. A hybrid deep learning based intrusion detection system using spatial-temporal representation of in-vehicle network traffic. Veh. Commun. 2022, 35, 100471. [CrossRef]

30. Ma, B.; Yang, S.; Zuo, Z.; Zou, B.; Cao, Y.; Yan, X.; Zhou, S.; Li, J. An Authentication and Secure Communication Scheme for In-Vehicle Networks Based on SOME/IP. Sensors 2022, 22, 647. [CrossRef]

31. Malina, L.; Srivastava, G.; Dzurenda, P.; Hajny, J.; Fujdiak, R. A Secure Publish/Subscribe Protocol for Internet of Things. In Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES 2019), Canterbury, UK, 26–29 August 2019.

31. Moulahi, T.; Zidi, S.; Alabdulatif, A.; Atiquzzaman, M. Comparative Performance Evaluation of Intrusion Detection Based on Machine Learning in In-Vehicle Controller Area Network Bus. IEEE Access 2021, 9, 99595–99605. [CrossRef]

32. Mun, H.; Han, K.; Lee, D.H. Ensuring safety and security in CAN-based automotive embedded systems: A combination of design optimization and secure communication. IEEE Trans. Veh. Technol. 2020, 69, 7078–7091. [CrossRef]

33. Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. IEEE Commun. Surv. Tutor. 2019, 21, 2702–2733. [CrossRef]

34. Noor, M.b.M.; Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. Comput. Netw. 2019, 148, 283–294. [CrossRef]

35. Pekaric, I.; Sauerwein, C.; Haselwanter, S.; Felderer, M. A taxonomy of attack mechanisms in the automotive domain. Comput. Stand. Interfaces 2021, 78, 103539. [CrossRef]

36. Radoglou Grammatikis, P.I.; Sarigiannidis, P.G.; Moscholios, I.D. Securing the Internet of Things: Challenges, threats and solutions. Internet Things 2019, 5, 41–70. [CrossRef]

37. Riahi Sfar, A.; Natalizio, E.; Challal, Y.; Chtourou, Z. A roadmap for security challenges in the Internet of Things. Digit. Commun. Netw. 2018, 4, 118–137. [CrossRef]

38. Saint-Andre, P. Extensible Messaging and Presence Protocol (XMPP): Core. Available online: https: //tools.ietf.org/html/rfc6120 (accessed on 15 March 2023).

39. Shelby, Z.; Hartke, K.; Bormann, C. The Constrained Application Protocol (CoAP). Available online: https://tools.ietf.org/html/rfc7252 (accessed on 15 March 2023).

40. Song, H.M.; Kim, H.K. Self-supervised anomaly detection for in-vehicle network using noised pseudo normal data. IEEE Trans. Veh. Technol. 2021, 70, 1098–1108. [CrossRef]

41. Sun, X.; Yu, F.R.; Zhang, P. A survey on cyber-security of connected and autonomous vehicles (CAVs). IEEE Trans. Intell. Transp. Syst. 2021, 23, 6240–6259. [CrossRef]

42. Walrand, J.; Turner, M.; Myers, R. An architecture for in-vehicle networks. IEEE Trans. Veh. Technol. 2021, 70, 6335–6342. [CrossRef]

43. Xie, G.; Yang, L.T.; Liu, Y.; Luo, H.; Peng, X.; Li, R. Security enhancement for real-time independent in-vehicle CAN-FD messages in vehicular networks. IEEE Trans. Veh. Technol. 2021, 70, 5244–5253. [CrossRef]

44. Youn, T.Y.; Lee, Y.; Woo, S. Practical sender authentication scheme for in-vehicle CAN with efficient key management. IEEE Access 2020, 8, 86836–86849. [CrossRef]

45. Zhang, L.; Ma, D. A Hybrid Approach Toward Efficient and Accurate Intrusion Detection for In-Vehicle Networks. IEEE Access 2022, 10, 10852–10866. [CrossRef]