CYBERSECURITY E IMPRESE ISTRUZIONI PER L'USO

Di Dario Merletti

F D A
Fastweb Digital Academy

Fastweb Digital Academy

la tua scuola per le professioni del Futuro

Siamo una scuola digitale che offre a giovani e adulti formazione specialistica sulle professioni digitali.
La nostra missione è quella aiutarti ad affrontare con fiducia il mercato del lavoro che richiede sempre più specifiche competenze digitali. Puoi arricchire il tuo percorso professionale digitale attraverso i nostri molteplici corsi orientati specificatamente alle nuove professioni del futuro.

Ogni corso adotta un approccio informale ed esperienziale e sono tenuti da specialisti e professionisti del settore. Al termine di ogni corso viene rilasciato a chi supera il test sulle competenze acquisite un open badge (attestato di partecipazione digitale).

Il corso "Cybersecurity e Imprese: istruzioni per l'uso" fa parte della nostra sezione On Demand. Ogni video lezione è accompagnata dalle slides preparate dal docente del corso esclusivamente per Fastweb Digital Academy.

Abbiamo preparato per te uno Student's Kit che rappresenta un insieme delle informazioni che ti permetteranno in qualsiasi momento di seguire al meglio i corsi On Demand.

Ti auguriamo buon Futuro!


@fastwebdigitalacademy


@FastwebDigitalAcademy


@fwdigitalacademy

#getdigital

Dispensa del corso "CYBERSECURITY E IMPRESE ISTRUZIONI PER L'USO"

Lo scenario di riferimento

Qualche domanda preliminare

Cosa si intende per Cybersecurity?

La cybersecurity è **la difesa** di un sistema informatico rispetto ad azioni mirate ad **ostacolarne o alterarne il funzionamento**, o ad **alterare o carpire i dati** in esso contenuti.

La Cybersecurity è un tema per esperti?

La Cybersecurity **riguarda tutti** perché **la nostra vita privata e professionale è sempre più digitale.**

Il Digitale è "diffuso"

Nella vita privata

Notiziari, *social media*, messaggistica, acquisti e *home banking*, navigazione stradale, studio, rapporti con le pubbliche amministrazioni.

Sul lavoro

Elaborazione dati, produzione di documenti o contenuti, gestione della produzione, rapporti con altre organizzazioni, utenti, clienti, dipendenti.

Nei servizi e nelle infrastrutture

Trasporti, energia, acqua, sanità, distribuzione beni di consumo.

I Dati: un po' di lessico

Riservatezza

Un dato è **noto solo a un insieme di persone**

Integrità

Un dato **non è stato alterato**

Disponibilità

Un dato **è disponibile all'accesso** o all'uso

Conosciamo davvero il Web?

SURFACE WEB

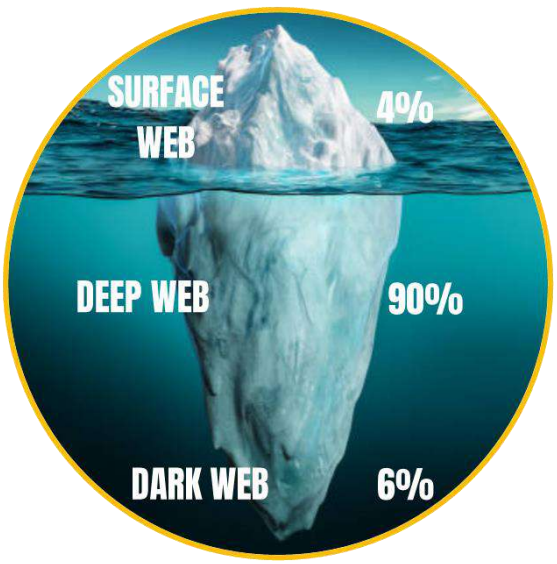
Parte di rete internet «navigabile» con browser e **raggiungibile tramite motori di ricerca** (Google, Bing...)

DEEP WEB

Parte di rete non «indicizzata» cioè non raggiungibile con motori di ricerca (es. contenuti generati da utenti come forum privati, gruppi Facebook, documenti di uso settoriale - legali, scientifici, governativi, ecc.)

DARK WEB

Parte di rete internet «oscura»; **accedibile solo con strumenti specifici** che **cela anche attività illecite e criminali.**



Fonte: Fastweb

Chi ci minaccia ?

84%: crimine organizzato

- fine: profitto economico
- bersagli: privati cittadini, organizzazioni e imprese

12%: forze militari e intelligence

- fine: pressione verso altri paesi, guerra, spionaggio
- bersagli: organizzazioni / infrastrutture / forze militari di altri paesi

1%: soggetti motivati politicamente

- fine: dimostrazione, diffusione di messaggi
- bersagli: istituzioni, imprese

3%: attacchi non attribuibili

Fonte: Paolo Passeri, hackmageddon.com

Cybercrime: un'attività dannosa

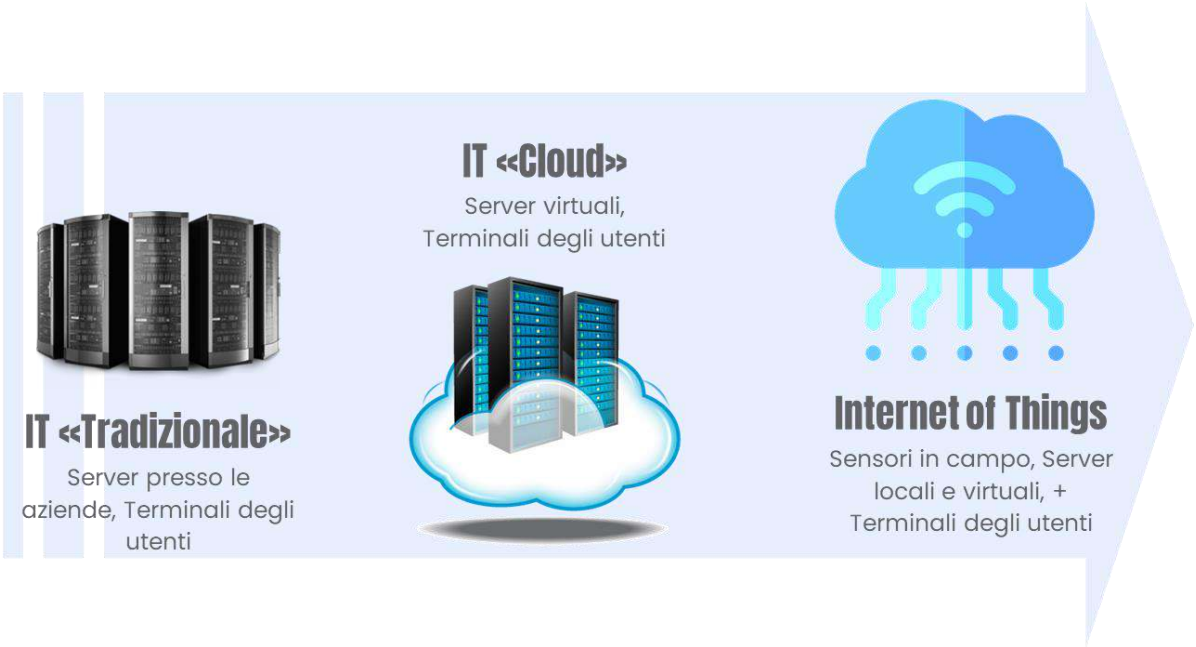
WORLD ECONOMIC FORUM

...In 2021, according to Cybersecurity Ventures, cybercrime damages might reach **US$6 trillion**...

Fonte: World Economic Forum - The Global Risks Report 2020

Imprese da difendere

Un perimetro sempre piu' esteso

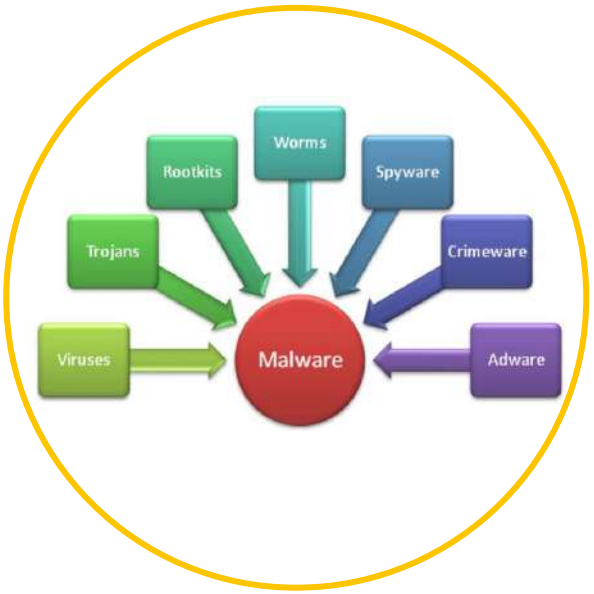


Le minacce

Alcune tipologie di attacco

MALWARE

Malicious software, indica un qualsiasi programma informatico usato per disturbare le operazioni svolte da un computer, rubare informazioni sensibili, accedere a sistemi informatici privati, o mostrare pubblicità indesiderata..



Ransomware famosi:
Cryptolocker, Wannacry
Petya

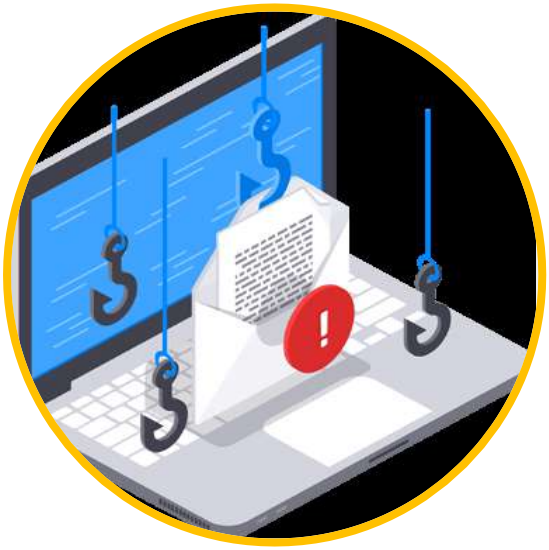
RANSOMWARE

- **Tipo di malware** che limita l'accesso del dispositivo che infetta, richiedendo un riscatto da pagare per rimuovere la limitazione.

- Alcune forme di ransomware bloccano il sistema e intimano l'utente a pagare per sbloccare il sistema, altri invece cifrano i file dell'utente chiedendo di pagare per riportare i file cifrati in chiaro.

0-DAY ATTACK

- **Vulnerabilità di sicurezza non pubblicamente nota** e il **relativo programma detto "exploit"** che sfrutta questa vulnerabilità per eseguire azioni illecite nel sistema infettato



PHISHING

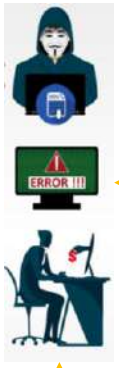
- Tipo di **truffa effettuata su Internet** attraverso la quale un **malintenzionato si finge un ente affidabile** in una comunicazione digitale e **inganna la vittima** convincendola a **fornire informazioni personali, dati finanziari o codici di accesso**.

- Il malintenzionato invia **messaggi di posta elettronica che imitano comunicazioni legittime** di fornitori di servizi, personalizzandoli verso le potenziali vittime con informazioni ottenute attraverso tecniche **di ingegneria sociale**.

Phishing

Esempi

Email con allegato o link malevolo



Il Cybercriminale invia ad un account aziendale un **messaggio email con un allegato** che contiene un software «malevolo»o direttamente un «ransomware»

Aperto l'allegato, il software malevolo viene eseguito e le **conseguenze** sono il **furto di informaazioni** o la **richiesta di riscatto**.

Business Email compromise

Il **Cybercriminale «impersonifica» un account email aziendale**, usa cioè un'identità «rubata» e **fa una richiesta formalmente legittima**, es. variazione pagamento

La richiesta è **ritenuta corretta** e **viene eseguita...**

Come opera il Cybercrime

FASE 1 - STUDIARE LE VITTIME POTENZIALI

- I Cybercriminali utilizzano un **approccio «massivo»** (pesca industriale) ma molto sofisticato servendosi di tecnologie basate su **Intelligenza Artificiale** che «esaminano» enormi quantità di dati.
- Collezionano il maggior numero possibile di informazioni sulle potenziali vittime ad esempio con attività di **INGEGNERIA SOCIALE** cioè con lo **studio del comportamento delle persone attraverso le tracce digitali** lasciate per carpire informazioni confidenziali.

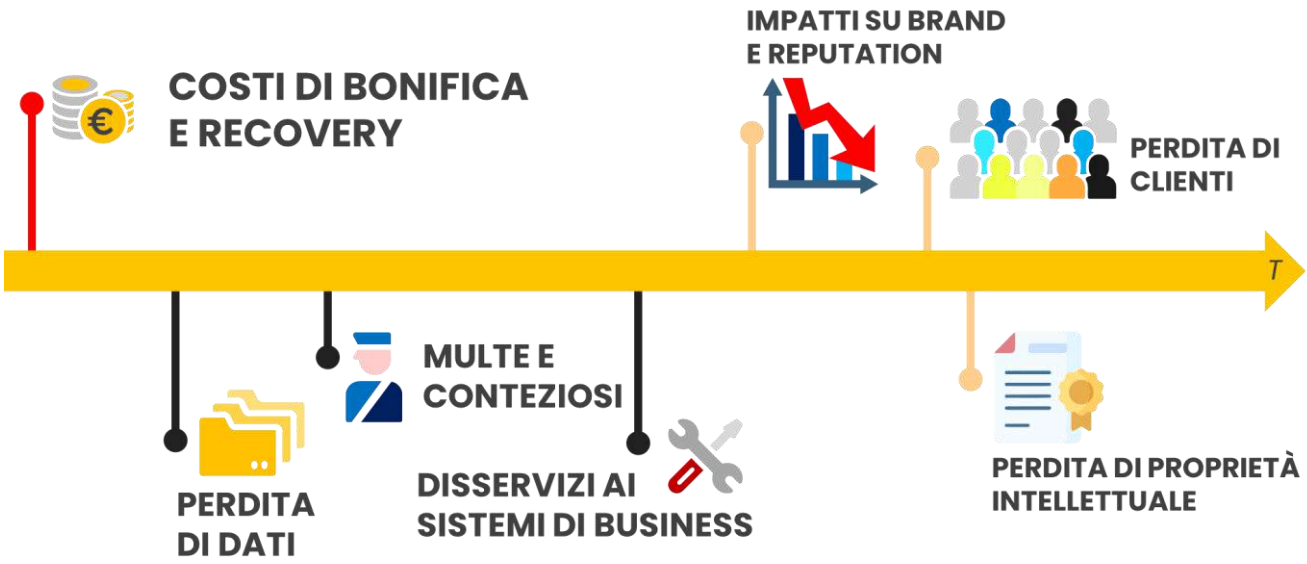
FASE 2 - SELEZIONARE LE VITTIME

- Grazie alle informazioni carpite **i cybercriminali effettuano un vero e proprio assessment delle vittime** «selezionando» quelle per le quali il rapporto costi/benefici risulti favorevole.
- Sono «privilegiati» obiettivi per i quali si scopre per esempio, **un'infrastruttura più vulnerabile o meno protetta** o **utenti per i quali si dispone di molte informazioni** che possono massimizzare il successo di una campagna di phishing ad esempio.

FASE 3 - ATTACCO QUASI A "COLPO SICURO"

- Dopo tutta l'attività preparatoria del «target» i cybercriminali sferrano l'attacco
- Tipicamente utilizzano **mail di phishing** sempre più personalizzate e sofisticate costruite basandosi sulle informazioni precedentemente raccolte per essere sempre più verosimili e credibili agli occhi della vittima.

Conseguenze pesanti



Valutare i rischi

Comprendere i fattori di rischio

LE PERSONE

CONSAPEVOLEZZA NELLA POPOLAZIONE AZIENDALE DEI RISCHI CYBER

TECNOLOGIE

INFORMATION E OPERATION TECNOLOGY

Comprendere i fattori di rischio

LE PERSONE

85% degli incidenti gravi ha una componente «umana»

- Uso scorretto di credenziali e password
- Scarsa attenzione alle E-mail (mittente, contenuto, allegati…)
- Utilizzo "disinvolto" dei social network e delle informazioni personali che vi circolano

Fonte: Fastweb

Comprendere i fattori di rischio

TECNOLOGIE

VULNERABILITY ASSESSMENT

- **Ricerca** di vulnerabilità ovvero "**punti di debolezza**" nelle applicazioni che "girano" nella nostra rete e che possono essere sfruttati da un Cybercriminale.

- Può essere un **servizio gestito** e, in parte, anche automatizzato **acquistabile sul mercato.**

- Di solito è **corredato con report** che riportano indicazioni utili per risolvere i problemi rilevati, generalmente tramite attività di **aggiornamento del software** (PATCHING).

PENETRATION TEST

- **Prova di intrusione effettiva** condotta da un Ethical Hacker, cioè un esperto di cybersecurity che conosce le tecniche dei cybercriminali e nella pratica "forza" le difese per testarle

- **E' un'attività** delicata **che deve essere condotta da soggetti altamente specializzati** e di assoluta fiducia.

Quanto il rischio è elevato?

CAPIRE I "SEGNALI DEBOLI" PRESENTI NEL DARK WEB

- **THREAT INTELLIGENGE: servizi di "ascolto" del Dark Web** in cui sono ricercate informazioni come credenziali, indirizzi mail, ecc. che possono essere sfruttate da cybercriminali per scagliare un attacco (es. mail di phishing)
- Sono gestiti da **operatori altamente specializzati** che, attraverso veri e propri servizi di intelligence, sono in grado di individuare informazioni e segnali che fanno presagire possibili attacchi e consentono di predisporre adeguate contromisure (es. cambio psw.)

Quantificare i possibili danni

BUSINESS IMPACT ANALYSIS

- **Quanto costa fermare**, magari per diversi giorni/settimane **processi o reparti vitali** come la produzione, o l'amministrazione?
- **Quanto costa recuperare le informazioni** non più disponibili?
- Possono essere sottratte informazioni personali o sensibili con possibili sanzioni per violazioni del GDPR? **Il vertice dell'azienda è responsabile in prima persona.**
- Quanto è probabile che tutto ciò accada?

Mitigare i rischi

Definire una strategia di mitigazione del rischio Cyber

Una **STRATEGIA DI MITIGAZIONE DEL RISCHIO** adeguata coinvolge diversi ambiti:

- **ORGANIZZAZIONE e PROCESSI**
  - **FORMAZIONE** (SECURITY AWARENESS)
  - **ASSICURAZIONI** PER RISCHIO CYBER
- **TECNOLOGIA**
  - **SERVIZI E TECNOLOGIE DI PROTEZIONE**

Organizzazione

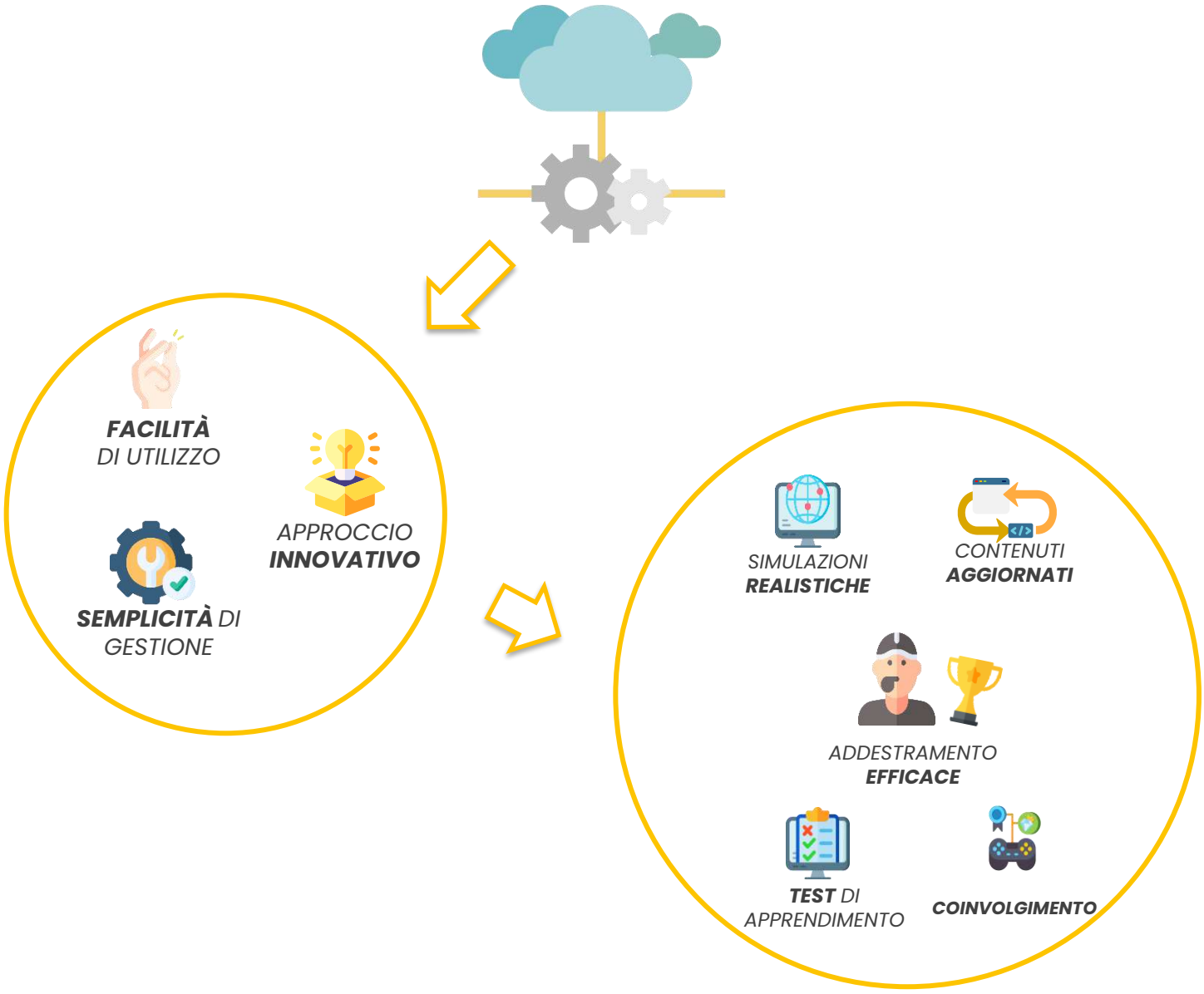
FORMAZIONE DEL PERSONALE

È attraverso una **formazione efficace** che si possono **trasformare i comportamenti** delle persone per renderle all'altezza della minaccia

Organizzazione

FORMAZIONE DEL PERSONALE IN PRATICA

PIATTAFORMA
SECURITY AWARENESS



Tecnologia

SERVIZI E TECNOOGIE DI PROTEZIONE

Accesso sicuro da/verso il Web

ESIGENZE

- **Navigazione internet protetta** (es. esclusione siti web potenzialmente pericolosi) e **protezione della rete aziendale.**

- Accesso dal WEB ad un **sito aziendale sicuro** (es. E-commerce)

SOLUZIONI

- **Next generation firewall e UTM (Unified Threat Mangement) -** Dispositivo HW o SW che integra diverse funzionalità di sicurezza.

- **Web Application Firewall -** Filtra, effettua il monitoring e blocca il traffico verso le applicazioni aziendali «esposte» sul Web.

Accesso sicuro da/verso il Web

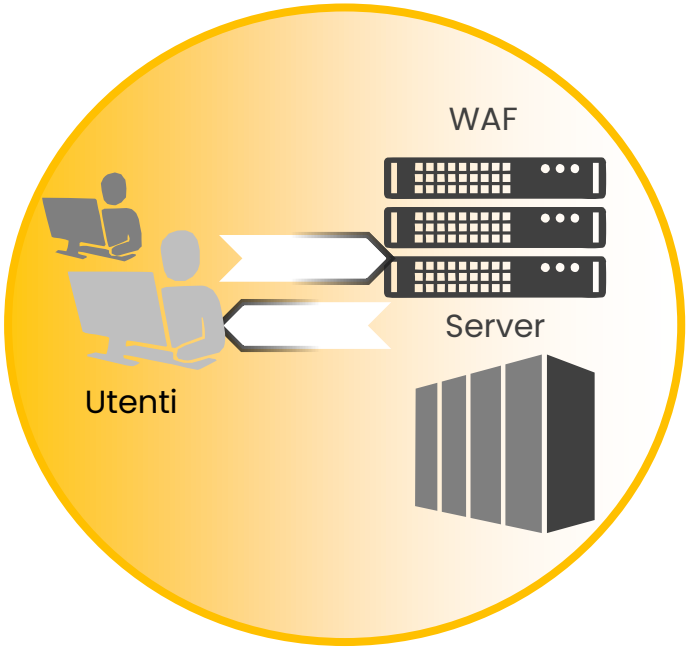
NEXT GENERATION FIREWALL e UTM

Firewall in grado di **bloccare tentativi di attacco in maniera unificata** tramite:

- Analisi dei pacchetti a livello applicativo DPI (Deep-Packet Inspection)
- Rilevamento e prevenzione delle intrusioni IDS/IPS (Intrusion Detection System/Intrusion Prevention System)
- Identificazione dell'utente
- Definizione di regole specifiche per ogni applicazione e per utenti (Application Policy)

WEB APPLICATION FIREWALL (WAF)

- Si differenzia rispetto agli altri tipi di firewall perché **è uno strumento progettato per proteggere specificamente dati e applicazioni esposte sul WEB** (siti istituzionali, Web server, Web Mail, E-commerce ecc.).
- **Interpreta il contenuto delle richieste web** ed **è in grado di prevenire gli attacchi** definiti nella Top 10 OWASP (Open Web Application Security Project).



Proteggere i dati

ESIGENZE

- **Fronteggiare i malware** che hanno i dati come obiettivo (es. ransomware).

- Conoscere **chi** sta accedendo a sistemi e dati e **quando**.

- **Prevenire un'uscita non autorizzata** di dati e informazioni.

SOLUZIONI

- **Anti malware avanzati (EPP – Enpoint Protection**: sono l'evoluzione degli antivirus con elevate capacità di mitigazione grazie all'AI.
- **Identity Access Management** (IAM): conoscere e poter autorizzare l'accesso a sistemi e informazioni anche in cloud.
- **Data Loss Prevention** (DLP) classificare documenti/utenti e controllarne l'accesso e le possibili azioni.

Proteggere i dati

ANTI MALWARE AVANZATI (EPP - Endpoint Protection)

Sono **l'evoluzione degli antivirus:**

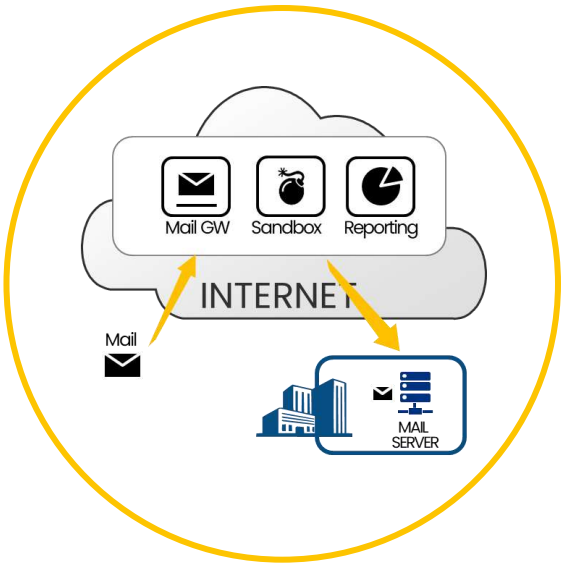
- Non si limitano a identificare e isolare malware già noti.
- Hanno elevate capacità di mitigazione grazie **all'analisi comportamentale** basata su AI.
- Proteggono da **virus tradizionali** e da **attacchi 0-Day**

Proteggere il servizio di posta elettronica

Sono disponibili sul mercato diversi servizi, tipicamente erogati dal Cloud, che consentono di analizzare il traffico mail da/per l'azienda e intervenire a diversi livelli:

- Tipicamente un **mail GW** eroga **funzionalità classiche antispam/antivirus basate su minacce note**

- si possono aggiungere **funzionalità più evolute** in grado di **individuare minacce sofisticate** (es. ransomware o 0-Day) attraverso l'esecuzione di file sospetti in un ambiente isolato (es Sandbox).



Poter ripartire dopo un attacco

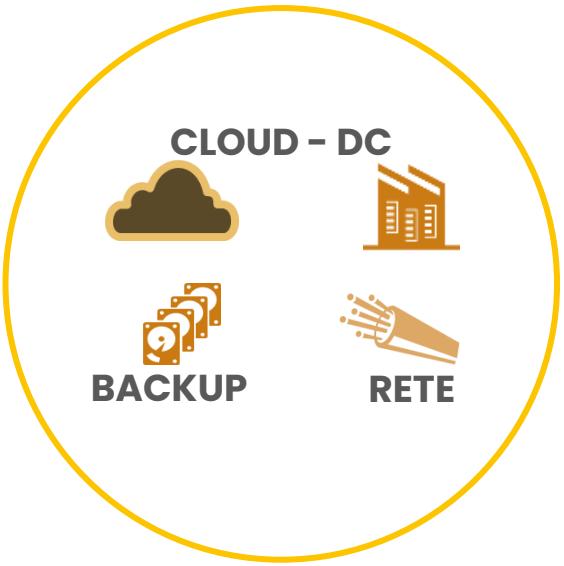
Continuità operativa: backup e disaster recovery

Per garantire una ripartenza con la minima perdita di informazioni e di tempo occorre prevedere:

- **processi** e **procedure di backup** continuativo dei Dati

- diponibilità di **applicazioni allineate in tempo utile**

- Il **cloud è una scelta consigliabile** per entrambi gli aspetti e sono anche disponibili sul mercato **servizi DRaaS** (Disaster Recovery as a Service)



@fastwebdigitalacademy

@FastwebDigitalAcademy

@fwdigitalacademy

#getdigital

F D A

Fastweb Digital Academy