Guida introduttiva alla sicurezza informatica

Documento per uso informativo, formativo e divulgativo a beneficio di tutti coloro che, non avendo particolari competenze e conoscenze informatiche, vogliono saperne di più sul mondo della cybersecurity, con tutte le implicazioni per la vita professionale e personale che comporta.

La lettura è consigliata al personale delle aziende e delle Pubbliche Amministrazioni che non si occupa direttamente di informatica.

Computer Care SRL

2021

www.computercare.it

https://www.linkedin.com/company/computer-care-srl/

SOMMARIO

1. Panoramica sulla cybersecurity: conoscere di cosa si sta parlando 3
1.1. Infrastrutture informatiche e di TLC 3
1.1.1. Reti informatiche 4
1.1.2. Reti cablate 5
1.1.3. Reti senza fili (WI-FI) 6
1.1.4. Rete cellulare 7
1.1.5. Router 8
1.1.6. Firewall 9
1.1.7. VPN 10
1.1.8. Backup 11
1.1.9. Cloud 12
1.1.10. Antivirus 13
1.2. Cybercrime perché e come avvengono gli attacchi 14
1.2.1. Numeri e diffusione del fenomeno 16
1.2.2. Il fattore umano 17
1.2.3. Virus e malware 18
1.2.4. Spamming e phishing 19
1.2.5. Social engineering 21
1.2.6. Ransomware 22
1.2.7. Attacchi tipo brute force 23
1.2.8. Vulnerabilità dei software 24
2. Minacce e rischi legati alla Cybersecurity 25
2.1. I rischi che le persone corrono on line 25
2.1.1. Cyberbullismo 26
2.1.2. Revenge porn, pedopornografia 27
2.1.3. Grooming o adescamento on line 28
2.1.4. Sexting 28
2.1.5. Sextortion 29
2.1.6. Cyberstalking 29
2.1.7. Hating 30
2.1.8. Furto d'identità e credenziali 31
2.1.9. Carte di pagamento e conti on line 32
2.1.10. Dipendenza da internet/social 33

2.2. Panoramica dei rischi da cybercrime per l'azienda 34
2.2.1. Data breach 35
2.2.2. Failure data 36
2.2.3. Data corruption 37
2.2.4. Dati personali e sensibili 38
2.2.5. Truffe contro il patrimonio 39
2.2.6. GDPR 40
2.2.7. Linee guida AGID per la PA 41
3. Buone pratiche per difendersi dal Cybercrime 42
3.1. Cosa fare in azienda 42
3.1.1. Gestione del rischio e difesa aziendale 42
3.1.2. Linee guida security per PMI 43
3.1.3. Backup dei dati aziendale e politiche di conservazione dei dati 44
3.1.4. Proteggere l'organizzazione da virus, malware, ecc. 45
3.1.5. Mantenere sicuri smartphone e tablet 46
3.1.6. Policy di password management 47
3.1.7. Proteggersi dal phishing e dal thief information 48
3.1.8. Cosa fare se … il ruolo della Polizia postale 49
3.2. Cosa fare personalmente in più 50
3.2.1. Bloccare l'accesso ai propri dispositivi 50
3.2.2. Backup dei dati personali 51
3.2.3. Gestione delle proprie password 52
3.2.4. Aggiornamenti di sistema per la sicurezza dei dispositivi 53
3.2.5. Difendersi dal phishing 54
3.2.6. Proteggere la propria casella email 55
3.2.7. Proteggere i propri dati sui social network 56

1. Panoramica sulla cybersecurity: conoscere di cosa si sta parlando

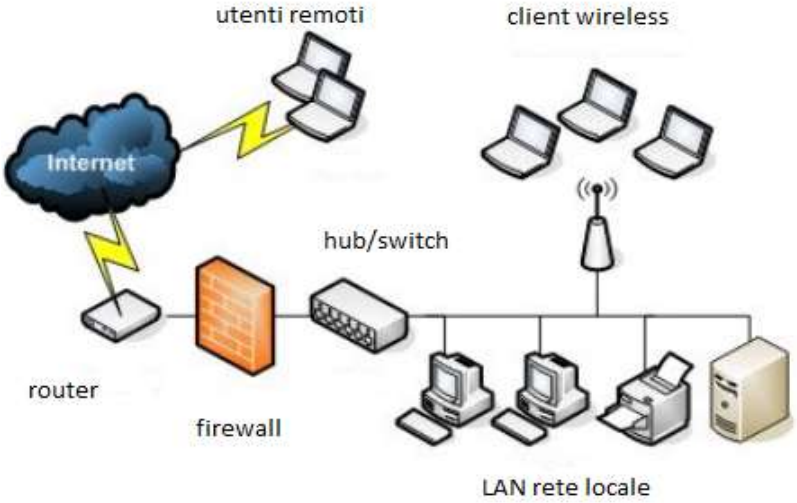
1.1. Infrastrutture informatiche e di TLC

Nei paragrafi successivi forniamo una veloce panoramica su quali sono le principali infrastrutture e dispositivi che, a vario titolo sono coinvolti nelle dinamiche della sicurezza informatica.

1.1.1. Reti informatiche

Una rete informatica è un insieme di dispositivi hardware sui quali sono installati dei software e collegati tra loro attraverso delle connessioni che permettono di scambiare risorse e dati.

L'hardware è la componente fisica di un dispositivo elettronico come un computer, uno smartphone, un router, una stampante; il software è invece l'insieme di programmi ed istruzioni che consentono ai dispositivi di svolgere determinate funzioni. Dispositivi che sono in qualche modo connessi ed in grado di scambiare dati ed informazioni tra loro fanno parte di una rete. All'interno di una rete i server, computer di solito molto potenti, elaborano dati e fanno girare software per fornire un servizio ad altri dispositivi collegati detti client quali altri computer o smartphone.



Le reti, che possono essere cablate o senza fili (wireless) si distinguono secondo criteri di estensione geografica in:

- LAN: Local Area Network ossia una rete interna di una struttura fisicamente o logicamente circoscritta (come un'azienda o un'abitazione) dove vengono condivise risorse hardware e software presenti all'interno della rete stessa;
- WAN: Wide Area Network ossia una rete estesa, senza limitazioni geografiche che collega risorse hardware e software teoricamente distribuite in tutto il mondo e facenti parte di altre LAN e WAN.
- Internet è la WAN più estesa e conosciuta di tutte.

La capacità di memoria di un dispositivo si misura in byte (=8 bit), quindi potremo avere computer con dischi da 2 TB o smartphone con memoria da 128 GB; la velocità delle reti dati, incluso la propria connessione ad internet fissa o mobile, si esprime invece con la quantità di dati che possono essere trasferiti in un secondo: bit/s, ed i suoi multipli Kb (Kilobit)/s, Mb (Megabit) /s, Gb (Gigabit)/s, ecc.

1.1.2. Reti cablate

Le reti informatiche con cavo, dette Ethernet utilizzano i cavi per collegare fisicamente i vari dispositivi tra loro. Ad ogni capo del cavo sono presenti dei connettori, detti RJ45, che servono per fissarlo al dispositivo e garantire la connessione dei contatti. Normalmente una rete cablata è veloce, affidabile e sicura ed è utilizzata per connettere i vari dispositivi all'interno di un ufficio o di un edificio. È tuttavia penalizzata dalla necessità di stendere i cavi per collegare i vari ambienti ed i computer all'interno di essi, anche attraverso l'utilizzo delle prese di rete a muro. Il fatto di avere un'infrastruttura fisica rende quindi la rete meno flessibile in caso di ristrutturazioni o riallestimenti di uffici con spostamento di pareti e postazioni.

I cavi si dividono in categorie per la lunghezza massima in cui possono trasmettere i dati ad una certa velocità secondo lo schema:

Categoria	MHz	Ethernet	Lunghezza massima del cavo
5e	100Mhz	100/1000Mbit/sec	100m
6	250Mhz	10Gbit = 10.000Mbit	100m
6a	500Mhz	10Gbit	da 37m a 55m
7	600Mhz	10Gbit	100m
7a	1000Mhz	10Gbit / 40Gibt / 100Gbit	100m / 50m / 15m

Il cavo può essere schermato o meno a seconda della presenza di una protezione, detta appunto schermatura, tra la guaina esterna e gli 8 cavetti divisi in quattro coppie (doppini) di fili al suo interno. I cavi schermati proteggono meglio la trasmissione dei dati dalle interferenze elettromagnetiche.

1.1.3. Reti senza fili (WI-FI)

Wi-Fi (Wireless Fidelity) è un insieme di tecnologie per reti locali senza fili basato su standard internazionali (IEEE 802.11), che consente a più dispositivi (per esempio personal computer, smartphone, tablet, Smart TV, ecc.) di essere connessi tra loro tramite onde radio e scambiarsi dati.

I dispositivi compatibili Wi-Fi possono connettersi ad internet attraverso un punto di accesso wireless denominato access point (AP che avrà alle sue spalle una rete cablata WLAN) o tramite un hotspot (che possiamo attivare, ad esempio, tramite uno smartphone e con il quale condividiamo l'accesso ad internet dello smartphone stesso). La portata di un segnale distribuito da un access point o da un hotspot è generalmente di circa 20 metri in un ambiente chiuso dove i muri e altre interferenze attenuano il segnale che, in campo aperto, potrebbe raggiungere anche di 100 metri.

Per accedere alla rete Wi-Fi si utilizzano dei protocolli di crittografia dei segnali radio emessi che consentono di renderli non comprensibili a chi non è in possesso delle chiavi di codifica. Un sistema moderno e diffuso è il WPA2 (Wi-Fi Protected Access).

Un altro sistema molto diffuso è il Wi-Fi Direct che permette a due o più dispositivi compatibili con tale tecnologia, di connettersi direttamente l'un l'altro senza usare una rete WiFi tradizionale (domestica o aziendale). Ogni dispositivo collegato diventa un access point wireless (Wi-Fi AP) rispetto agli altri dispositivi della rete che si viene a creare. L'accoppiamento dei dispositivi Wi-Fi Direct può avvenire tramite connessioni NFC (Near-Field Communication), con cui i dispositivi si scambiano le credenziali, oppure con la pressione di un tasto su uno o tutti i dispositivi, per autorizzare la connessione. Il Wi-Fi Direct può prendere il posto delle connessioni Bluetooth per le applicazioni che non si affidano a BLE (Bluetooth Low Energy) per contenere i consumi energetici.

Standard Wi-Fi	Reti	Velocità massima teorica
Wi-Fi 1	802.11b	11 Mbps
Wi-Fi 2	802.11a	54 Mbps
Wi-Fi 3	802.11g	54 Mbps
Wi-Fi 4	802.11n	450 Mbps
Wi-Fi 5	802.11ac	866 Mbps
Wi-Fi 6	802.11ax	1,2 Gbps

1.1.4. Rete cellulare

La rete cellulare è l'insieme di tecnologie in grado di consentire la connessione di smartphone ed altri dispositivi ad una centrale (della cella) attraverso onde radio ad una determinata frequenza. Questa connessione consente la trasmissione di dati e voce ad una determinata velocità. Attualmente le reti cellulari disponibili sono le seguenti:

- 2G (II generazione): standard **GSM**, velocità 9-14.4 kbps (Kilobit per secondo)
- 2,5G: standard **GPRS** (evoluzione del GSM), velocità 20-40 kbps
- 2,75G: standard **EDGE** (evoluzione del GPRS), velocità 60-180 kbps
- 3G (III generazione): standard **UMTS**, velocità 380-700 kbps
- 3,5G: tecnologia **HSDPA** e **HSPA+,** velocità 3,6-14,4 Mbps (Megabit per secondo)
- 4G (IV generazione): standard **VSF-Spread OFDM** e **LTE**, velocità fino a 150 Mbps (generalmente 20-30 Mbps)
- 5G: reti di telefonia mobile superiori alla tecnologia 4G/IMT-Advanced, velocità fino a 1000 Mbps (generalmente 200-300 Mbps).

Per collegarsi alle reti vengono utilizzate delle schede fisiche denominate SIM (Subscriber Identity Module) che sono delle smart card che, oltre ad essere identificate con il numero di telefono cellulare, permettono di archiviare al proprio interno anche il codice di identità internazionale di utente di telefonia mobile, l'IMSI (International Mobile Subscriber Identity).

Mini SIM - Micro SIM e Nano SIM (il perimetro più piccolo intorno alla smart card dorata)

La presenza di reti 5G in sempre più parti del territorio permette utilizzando un router 5G l'implementazione di una LAN ad alta/altissima velocità di trasmissione con un "collo di bottiglia" inevitabile che dipende dalla quantità di dati disponibile dal proprio piano tariffario. La quantità di dati inclusa nel piano tariffario include la somma totale delle quantità di dati da e verso l'operatore telefonico scelto.

1.1.5. Router

Un router è un dispositivo di rete usato come sistema di interfacciamento tra reti e sotto reti diverse (ad esempio dalla rete di casa o dell'ufficio alla rete internet) che permette di instradare le informazioni tra le varie reti (rete locale LAN e rete Internet ad esempio).

Questo è un router con access point (si nota dall'antenna) che collega una rete cablata, una rete WI-FI e la rete Internet (tramite collegamento DSL o **ADSL** in questo caso).

Molto diffusi sono i router che si connettono ad una rete cellulare 4G (come degli smartphone) e che permettono la connettività Internet tramite apposita SIM telefonica.

A sinistra in giallo un router cablato alla rete LAN - a destra in nero un router 4G che permette al router giallo di collegarsi ad internet tramite la rete cellulare.

La prerogativa sempre più diffusa è l'implementazione di numerosi servizi avanzati, un tempo riservati ad apparecchiature di costo ben maggiore, anche all'interno dei router di fascia **SOHO** (small office/home office).

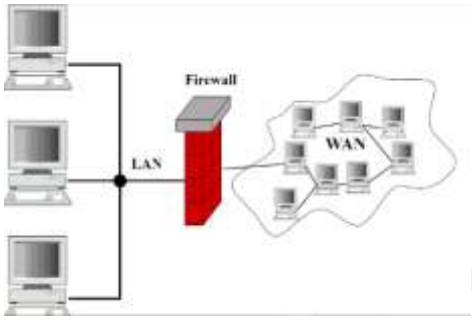
Nei moderni router sono presenti sia alcune prese RJ45 per la connessione di apparati via cavo (in giallo nel modello rappresentato in foto), sia antenne per la connessione via WiFi.

1.1.6. Firewall

Il firewall, dall'inglese muro tagliafuoco, è un dispositivo hardware e/o software per la difesa del canale di comunicazione tra reti a cui si applica. Al giorno d'oggi troviamo spesso delle **appliance** in cui un prodotto hardware ha un software integrato per svolgere le funzioni di firewall. Lo scopo del firewall è quello di filtrare il traffico dati che una rete (locale, interna, conosciuta e sicura) scambia con un'altra rete (tipicamente esterna, sconosciuta e insicura).

Un firewall filtra il traffico in base a due tipologie di **policy** (che possiamo tradurre con politiche o criteri):

1. Default-deny che significa che tutto il traffico è bloccato tranne quello esplicitamente permesso – metodo più sicuro ma complesso da implementare;
2. Default-allow che significa che tutto il traffico è permesso tranne quello che è esplicitamente vietato – metodo meno sicuro ma più semplice da implementare;



I firewall hardware presentano al loro interno un sistema operativo minimale con le funzionalità essenziali per il funzionamento invece di un sistema operativo completo (quindi con un numero maggiore di funzionalità e sotto-sistemi da controllare). Per via di questo spesso i firewall hardware risultano più sicuri dei firewall software anche se necessitano di una configurazione più complessa e articolata.

Una funzione spesso associata al firewall è la **NAT** (network address translation) che può aumentare la sicurezza di una rete mascherandone gli indirizzi IP all'interno.

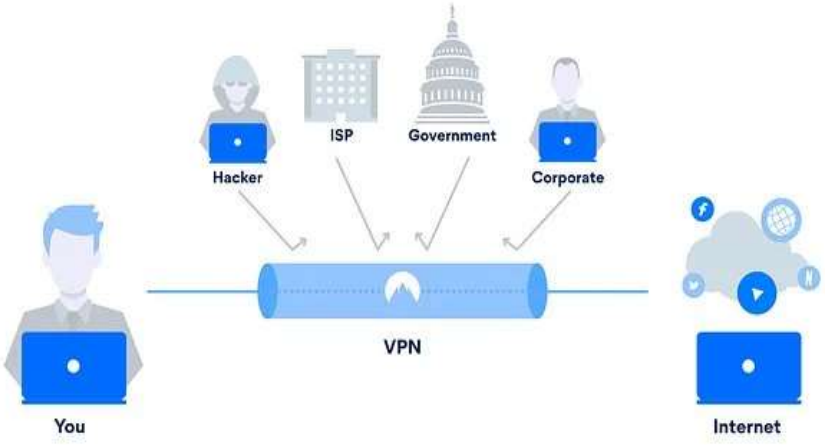
All'interno dei firewall troviamo anche strumenti software **IPS** (Intrusion prevention systems) che permettono di eseguire alcune azioni come mandare un allarme, eliminare pacchetti malevoli, resettare le connessioni e/o bloccare il traffico da un indirizzo IP attaccante.

I firewall si dividono in host-based (firewall software o personal firewall), come ad esempio quelli integrati nei sistemi operativi Windows,

e network-based (firewall hardware o firewall perimetrale).

1.1.7. VPN

La VPN (Virtual Private Network) è una rete di comunicazione privata che si realizza utilizzando come tecnologia di trasporto dei dati un sistema di trasmissione pubblico e condiviso, come ad esempio la suite di protocolli Internet. Semplificando potremmo dire che di fatto permette la realizzazione di una rete privata utilizzando l'infrastruttura di una rete pubblica (internet). Per poter raggiungere questo scopo il client si collega ad un server VPN che realizza una sorta di tunnel tra il client stesso e la risorsa o rete che si vuole raggiungere (ad esempio la propria rete aziendale). Questo permette al client (computer ma anche uno smartphone ad esempio) di utilizzare i servizi presenti sulla rete a cui si è collegati (file e cartelle condivise, stampanti ed altre risorse di rete) come se vi fosse un collegamento fisico diretto. Questo fa sì che reti separate e dislocate su un ampio territorio possano interagire come se fossero di fatto una LAN.



Per quanto riguarda le aziende una VPN ben strutturata può offrire diversi vantaggi:

- estende la connettività geografica fino a reti globali,
- migliora la sicurezza dove le linee di dati non sono state criptate,
- riduce i costi di operazione sui dati interni all'azienda,
- fornisce compatibilità con le reti a banda larga,
- fornisce un più veloce tempo di ritorno dell'investimento rispetto al trasporto tradizionale delle linee WAN (Wide Area Network)

Per quanto riguarda l'utente non aziendale la VPN permette di incapsulare il traffico dati dal proprio device al servizio a cui ci si collega rendendo di fatto più sicuro il traffico delle informazioni. Avvalersi di un servizio VPN attraverso una rete WLAN pubblica (Wi-Fi pubblico), ad esempio in aeroporto, permette di criptare i dati impedendo agli hacker la possibilità di accedere ai dati sensibili presenti sul device utilizzato (computer, smartphone, tablet).

1.1.8. Backup

Con il termine backup si intende la messa in sicurezza delle informazioni di un sistema informatico (o un semplice computer o smartphone) attraverso la creazione di una o più copie delle informazioni stesse (ridondanza). In caso di malfunzionamento per qualsivoglia motivo (evento accidentale o intenzionale, malevolo o semplice manutenzione) del device o sistema sorgente, queste copie dei dati serviranno per il recupero (ripristino) dei dati stessi.

Solitamente si effettua il backup per due scopi principali, primo di questi recuperare i dati nel momento in cui vengono persi, per esempio perché cancellati o corrotti. Il secondo è quello di recuperare i dati da un momento precedente, cioè utilizzare una versione precedente rispetto a quella attuale, di dati attualmente in possesso.
Qualsiasi strategia di backup inizia definendo un concetto di archivio (repository) dove i dati di backup devono essere organizzati e memorizzati.
Le principali tipologie di repository per back up sono:

- **Completo**; contiene immagini di sistema complete prese in uno o più specifici momenti nel tempo. Questa tecnologia è spesso utilizzata dai tecnici informatici per salvare un sistema configurato e perfettamente funzionante, quindi è generalmente più utile per la distribuzione di una configurazione standard per molti sistemi, piuttosto che come uno strumento per fare copie di backup in corso di sistemi diversi.
- **Incrementale**; punta a rendere minore l'occupazione dello spazio per la memorizzazione delle copie dei dati in base alle sole differenze che ci sono tra i dati in uso e quelli che sono già nel repository. Questo permette di eliminare le copie duplicate di dati rimasti invariati tra un backup ed il successivo. Tipicamente, un backup di tutti i file è realizzato una volta, o a intervalli, e serve come punto di riferimento per un set di backup incrementali successivi. Ripristinare l'intero sistema alla data dell'ultimo backup incrementale comporta di partire dall'ultimo backup completo, preso prima della perdita di dati, e quindi applicare ciascuno dei backup incrementali effettuati da allora.
- **Differenziale**; vengono salvati solo i dati che sono stati modificati dopo l'ultimo backup completo. Questo sistema ha il vantaggio che sono necessari solo un massimo di due insiemi per ripristinare i dati. Uno svantaggio, rispetto al metodo di backup incrementale, è che il tempo dall'ultimo backup completo (e quindi le variazioni cumulate di dati) aumenta via via, così come il tempo necessario per eseguire il backup differenziale.

Sempre più diffusi in ambito aziendale sono i NAS (Network Attached Storage), apparati che oltre a condividere servizi e file sulla rete includono al loro interno software di backup preinstallati ed alloggiamenti per hard disk.

1.1.9. Cloud

Il Cloud computing (nuvola) è una struttura di erogazione di servizi on-demand distribuita e scalabile normalmente integrata con la rete internet. La particolarità della struttura permette un bilanciamento dei carichi di lavoro lato server distribuendo l'impegno di risorse su più server a seconda della gravosità del carico istantaneo. Questo per esempio permette nel caso di pochi utenti collegati di usufruire della potenza di calcolo di anche un solo server ma, dinamicamente, al variare della domanda, ad esempio l'accesso di centinaia di nuovi utenti concomitanti, di chiamare in causa anche decine di altri server per "distribuire" il nuovo carico di lavoro richiesto.

Parlando di risorse e carico di lavoro si intendono assetti di tipo:

- Infrastrutturale come capacità di calcolo (processori), spazio di archiviazione dati (hard disk), connettività (velocità di trasferimento dati);
- Piattaforme per la gestione dei database (achivi di dati), controllo degli accessi, sicurezza delle informazioni, back up, ecc.;
- Applicativo come software per la posta elettronica, l'office automation (es. foglio elettronico), la collaborazione on line (es. video riunioni), la gestione dei contenuti.

Il fornitore dei servizi cloud rende disponibili delle risorse non più completamente ed appositamente dedicate e configurate per l'utente, ma rende solo parzialmente configurate dall'utente finale. Quando l'utente non utilizza la risorsa (ad esempio quando è disconnesso dalla rete), il sistema cloud in modo automatico ripristina la risorsa allo stato iniziale e permette in modo veloce ed economico di rivolgersi verso altre richieste di altri utenti.
Sfruttando la tecnologia del cloud gli utenti collegati al fornitore possono utilizzare i servizi offerti anche tramite un semplice browser Internet.

I servizi offerti per l'utente finale variano dallo spazio disco, alla capacità di calcolo, ai servizi di editing dei file di vario tipo. Di solito ci troviamo di fronte a servizi limitati (qualche GB di spazio disponibile) per gli account gratuiti che aumentano sottoscrivendo un upgrade del proprio account (a pagamento).

1.1.10. Antivirus

Un antivirus è un software finalizzato a prevenire, rilevare ed eventualmente rendere inoffensivi software e codici dannosi e malware per un computer come virus, spyware, trojan, worm, ransomware, ecc.

Attualmente i virus più diffusi si dicono polimorfi, in pratica software capaci di mutare il proprio codice in modo da ingannare gli antivirus durante l'analisi. Ogni volta che il virus infetta un file, lo fa con un codice leggermente differente da quello iniziale e quindi ogni nuova copia è diversa da quella precedente.

Un antivirus da solo, per quanto affidabile ed efficiente, non è una protezione completa contro la totalità dei virus informatici esistenti al mondo. Inoltre, un antivirus si basa su determinate regole e algoritmi scritti da esseri umani, e pertanto queste possono portare a errori come i falsi positivi, ossia file riconosciuti come infetti quando non lo sono, e falsi negativi, il caso opposto, oppure a decisioni sbagliate.

Un'ulteriore limitazione è dovuta al fatto che un virus potrebbe essere ancora non abbastanza diffuso, e quindi non essere ancora stato studiato da tutti i produttori di antivirus. La tecnologia euristica è una componente implementata da numerosi antivirus che consente di rilevare alcuni programmi maligni non noti all'antivirus, cioè non contenuti nel suo archivio di virus conosciuti. Viene generalmente utilizzata come tecnologia complementare al database incluso e costantemente aggiornato. Vi sono diversi tipi di tecnologie euristiche, quali ad esempio la scansione della memoria o del codice sorgente in cerca di pattern (schemi) noti come maligni.

Tuttavia, nonostante questo, il metodo dei signatures (firme lasciate dal virus) rimane uno dei metodi più efficienti e consolidati nell'industria del settore. Questo anche perché non tutti i malware si diffondono con la stessa rapidità e con la stessa intensità. Più un malware è infettivo, infatti, e più è probabile che sia arrivato nelle mani dei ricercatori delle aziende produttrici di software antivirus. Quindi, sebbene il metodo utilizzato non garantisca l'assoluta inviolabilità, assicura comunque una sicurezza abbastanza elevata dai malware più diffusi.

A titolo di esempio un elenco di alcuni tra i più noti antivirus commerciali:

- ESET NOD32 Antivirus
- Bitdefender Total Security 2021
- McAfee Antivirus Protection 2021
- Norton 360 Deluxe 2021 Antivirus
- AVG Ultimate 2021 AntivirusCleaner
- KASPERSKY INTERNET SECURITY 2020

1.2. Cybercrime perché e come avvengono gli attacchi

Il cybercrime o crimine informatico è una tipologia di crimine che include tutti gli utilizzi delle risorse, sia hardware sia software, al fine di produrre un risultato illecito che spazia dall'appropriarsi di dati sensibili altrui, all'utilizzo di software con intento diffamatorio, alla divulgazione di materiale pedopornografico, alla realizzazione di truffe e furti di denaro e a molti altri crimini.

Le motivazioni che portano ai crimini informatici sono sostanzialmente le stesse dei reati civili e penali trasferiti nel mondo informatico:

- reati contro la persona (diffamazione, furto d'identità)
- reati contro il patrimonio (furti, estorsioni)
- reati contro le istituzioni (interruzioni di servizio, spionaggio, controllo dei sistemi).

Per quanto riguarda le finalità di attacco, attualmente le più diffuse sono le truffe (es. phishing, compromissione di account email business) e l'estorsione (es. cryptolocker WannaCry in figura), a dimostrazione evidente di come il fine più comune del cybercrime sia la realizzazione di proventi economici attraverso attività illecite.

Altre finalità, meno comuni ma pur sempre degne di nota, riguardano:

- intrusione a scopo di spionaggio (es. politico, industriale, militare);
- interruzione di servizio (es. attacchi Dos – Denial of Service, DDos – Distributed Denial of Service);
- influenza e manipolazione dell'opinione pubblica (es. durante le elezioni);
- controllo di sistemi strategici o produttivi (es. centrali elettriche, impianti di produzione).

Considerando gli obiettivi degli attacchi, si osserva che i criminali informatici colpiscono (dati 2020) principalmente account email e social, portali di eCommerce, siti web aziendali ed istituzionali.

Nei prossimi anni si prevede che i principali obiettivi diverranno i dispositivi mobili, le infrastrutture critiche (es. reti elettriche, idriche e di telecomunicazioni), gli apparati smart home e smart building ed anche i veicoli connessi.

Per comprendere meglio i reati informatici occorre considerare, in aggiunta a quanto esposto precedentemente, anche l'impatto delle nuove tecnologie, dato che queste possono incrementare o favorire i cyber attacchi. Si parla di big data, cloud, smart objects – tutti sistemi che stanno migliorando i processi industriali e le vite delle persone. Ma queste tecnologie possono costituire anche un rischio per la sicurezza e per la privacy.

Uno dei trend digitali più significativi al momento è l'Intelligenza Artificiale, uno strumento utile per automatizzare il processo di raccolta e analisi dei dati e per gestire in maniera più efficace la sicurezza. Tuttavia, può costituire anche una minaccia e attrarre attacchi informatici: per esempio, possiamo pensare ad un utilizzo con intenti malevoli di algoritmi (sequenza di istruzioni da eseguire per risolvere un determinato lavoro) in grado di apprendere dal comportamento online degli utenti. A questo riguardo dobbiamo considerare la diffusione sempre più capillare degli oggetti intelligenti (smart objects) in casa (Amazon Echo, Google Home), che, essendo connessi alla rete e in grado di comprendere il linguaggio naturale, possono contribuire ad aumentare l'area e le possibilità di attacchi.

Nuovi rischi per la sicurezza sono legati anche al mondo dell'Internet of Things, come nel caso dei sensori collegati ai dispositivi OT (Operation Technology), utilizzati per il monitoraggio della produzione di beni. Oltre al contesto industriale, i criminali informatici possono colpire anche l'ambito privato, sfruttando dispositivi IOT compromessi in automobili e abitazioni.

Tra le minacce in aumento in ambito aziendale si individuano anche gli attacchi supply chain, mirati a danneggiare la catena del valore attraverso la violazione dei sistemi di un fornitore, di un partner o di un cliente di un'azienda al fine di accedere ai dati di quest'ultima. In futuro un ruolo importante sarà rappresentato anche dal cambiamento della sensibilità delle persone sul tema della privacy, nella condivisione di informazioni sui social network o nel fornire dati sensibili in cambio di servizi gratuiti.

Molte aziende stanno mettendo in atto azioni mirate a sensibilizzare i propri dipendenti sulla sicurezza informatica. Nonostante in molti casi siano previste policy e linee guida sul tema, spesso queste ultime vengono ignorate in maniera più o meno consapevole dai dipendenti.

Per gestire adeguatamente la sicurezza informatica, alle aziende non basta investire in tecnologie per la protezione dagli attacchi esterni, perché i rischi di vulnerabilità informatica possono provenire anche dall'interno. Infatti, spesso i cyber criminali non utilizzano tecniche sofisticate, bensì sfruttano le debolezze legate al comportamento umano per accedere alle informazioni delle aziende.

1.2.1. Numeri e diffusione del fenomeno

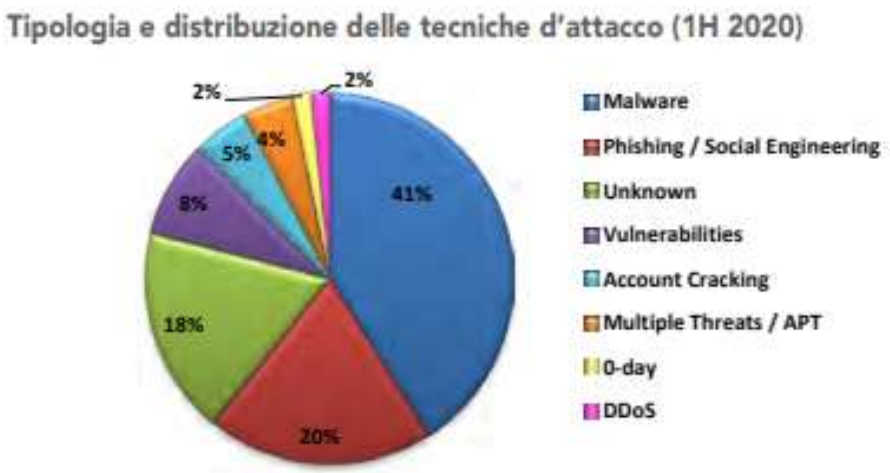
I numeri relativi al cybercrime sono in continuo e costante aumento soprattutto considerando la crescita esponenziale degli apparati connessi che si diffonde sempre più anche in settori fino a pochi anni fa non presenti (smart TV, elettrodomestici intelligenti, dispositivi wearable o indossabili, smart things).

Distribuzione generale delle tecniche di attacco (2014 – 1H 2020)

TIPOLOGIA TECNICHE DI ATTACCO	2014	2015	2016	2017	2018	2019	1H 2019	1H 2020	1H 20 su 1H 19	Trend
Malware	127	106	229	446	585	730	324	346	6.8%	
Unknown	199	232	338	277	408	317	166	153	-7.8%	
Known Vulnerabilities / Misconfig.	195	184	136	127	177	126	75	72	-4.0%	
Phishing / Social Engineering	4	6	76	102	160	291	134	169	26.1%	
Multiple Techniques / APT	60	104	59	63	98	65	40	38	-5.0%	
Account Cracking	86	91	46	52	56	86	33	41	24.2%	
DDoS	81	101	115	38	38	23	10	13	30.0%	
0-day	8	3	13	12	20	30	12	14	16.7%	
Phone Hacking	3	1	3	3	9	1	1	3	200.0%	
SQL Injection	110	184	35	7	1	1	1	1	0.0%	-

Alcuni dati con focus sul primo semestre del 2020 (Fonte Clusit – Associazione italiana per la sicurezza informatica) relative all'evoluzione delle tecniche di attacco utilizzate negli ultimi anni, vedono un aumento del numero di attacchi tramite malware, di tecniche di social engineering e phishing e della compromissione di account.

Le percentuali relative (Fonte Clusit) alla tipologia di attacco ci mostrano che quasi due attacchi su tre provengono da malware o da phishing/social engineering.



Secondo il Cybersecurity report 2020 di Trend Micro, l'Italia è quinta al mondo e prima in Europa per attacchi macro malware (programmi malevoli nascosti nelle macro dei documenti Word/Excel soprattutto) con un numero rilevato di oltre 13.000 attacchi. Il report evidenzia come il nostro paese sia uno dei più colpiti al mondo per quanto riguarda i malware: nel 2020 ne sono stati intercettati oltre 22 milioni. Siamo anche l'undicesimo Paese al mondo per numero di attacchi ransomware ricevuti. Nel solo 2020 sono state scaricate oltre 140.000 app maligne e sono stati visitati oltre 11 milioni di siti web maligni. Le minacce arrivate per mail sono oltre 300 milioni. Anche il settore bancario viene colpito con oltre 4.000 malware di online banking.

Siamo quindi di fronte a numeri impressionanti ed in costante crescita, il tasso della quale è destinato sicuramente ad aumentare con il diffondersi di nuovi apparati, tecnologie e servizi disponibili in rete.

1.2.2. Il fattore umano

Quando parliamo di fattore umano nel campo informatico andiamo ad evidenziare che le persone agiscono in modi prevedibili approcciandosi ai problemi che vengono loro posti, ma anche alle attività che svolgono nella loro quotidianità.

Relativamente al mondo informatico, ed in particolare nell'approccio delle persone rispetto alle problematiche tecnologiche, possiamo osservare queste modalità e caratteristiche diffuse:

- awareness (consapevolezza) – es. quando clicchiamo su un link all'interno di una mail riteniamo di saper riconoscere una mail legittima da una illegittima,

- fallibilità degli esseri umani,

- tendenza alla fiducia – es. se una mail arriva da un contatto conosciuto tendiamo a qualificarla per buona,

- l'utilizzo di interfacce/architetture complesse che richiedono aggiornamenti e formazione dedicata continua,

- prestazioni vs sicurezza – es. si preferisce rapidità di esecuzione invece di sicurezza nel processo,

- utilizzo Shadow IT (interfacce parzialmente nascoste agli amministratori della rete aziendale) o la presenza di soluzioni IT all'interno dell'organizzazione senza esplicito consenso dell'organizzazione stessa:

  - utilizzo di chiavette USB e HD esterni per il trasporto dei dati,
  - software per la messagistica online (WhatsApp desktop ad esempio),
  - Gmail ed altri servizi di posta online,
  - Google Docs ed altri sistemi di condivisione dei documenti,
  - Skype ed altri sistemi VOIP (Voice Over IP),
  - macro di Excel e database access,

- BYOD - Bring your own device – utilizzare il device personale (es. lo smartphone) in contesto professionale o aziendale.

La principale causa di violazioni e incidenti che riguardano le infrastrutture informatiche resta quindi il fattore umano, la vulnerabilità degli utenti finali e la loro debolezza, tipicamente umana, nel riconoscere ed evitare le trappole informatiche dei cyber criminali, rischiando di divenirne non solo vittima, ma anche complici inconsapevole.

Nessuna contromisura tecnologica o di processo è efficace contro il cybercrime se il corretto utilizzo ne è semplicemente disatteso, per negligenza, imprudenza, ignoranza o solo semplicemente per errore dalle singole persone.

1.2.3. Virus e malware

Malware (dall'inglese malicious software, "software malevole"), nella sicurezza informatica, definisce un programma informatico, di qualsiasi tipo, usato per alterare le operazioni svolte da un utente di un computer. È un software dannoso e malevolo, scritto e diffuso con l'obiettivo di danneggiare in qualche modo il sistema informatico che lo esegue e quindi uno o più utenti. I malware vengono comunemente chiamati virus informatici o semplicemente virus.

Un malware può essere creato con l'intento di arrecare danni ad un sistema informatico, per criptare i dati del computer della vittima, estorcendo denaro per la decriptazione (Cryptolocker), o per rubare di nascosto informazioni di vario tipo, da commerciali a private, senza essere rilevato dall'utente anche per lunghi periodi di tempo (es. Regin malware).

Il malware è suddivisibile in diverse tipologie differenti tra loro per scopi, modalità di diffusione e dannosità. Vediamo i principali:

- Virus, software o parti di essi che si installano all'interno di altri programmi ed ogni volta che vengono eseguiti (es. all'avvio anche automatico del programma infettato) si replicano.
- Worm, entrano nei sistemi informatici, modificano il sistema operativo del dispositivo infettato per replicarsi attraverso la rete, per diffondere un altro tipo di malware.
- Trojan horse, software lecito che all'interno contiene istruzioni dannose finalizzate a far prendere il controllo del dispositivo dai criminali informatici ad insaputa degli utenti.
- Spyware, servono per raccogliere e trasmettere all'esterno informazioni sul dispositivo infettato e sull'utente che lo utilizza (es. credenziali e password) a sua insaputa.
- Adware, malware che indirizzano la navigazione dell'utente su siti pericolosi e visualizzano, attraverso apertura di pagine e pop up, annunci pubblicitari anche fraudolenti.
- Keylogger, malware che, una volta installati sul dispositivo infettato registrano tutto quello che l'utente digita sulla tastiera e lo trasmettono all'esterno senza nessun malfunzionamento evidente.
- Ransomware, software che cripta tutti i dati presenti in memoria (dischi) o sulla rete locale del dispositivo infettato e li rende non più utilizzabili a meno del pagamento di un riscatto.

Molti attacchi informatici sfruttano backdoor (porte sul retro) di software applicativi legali, ossia delle vulnerabilità, più o meno conosciute dagli stessi sviluppatori, che consentono di evitare le consuete procedure di autenticazione ed accesso ai sistemi.

1.2.4. Spamming e phishing

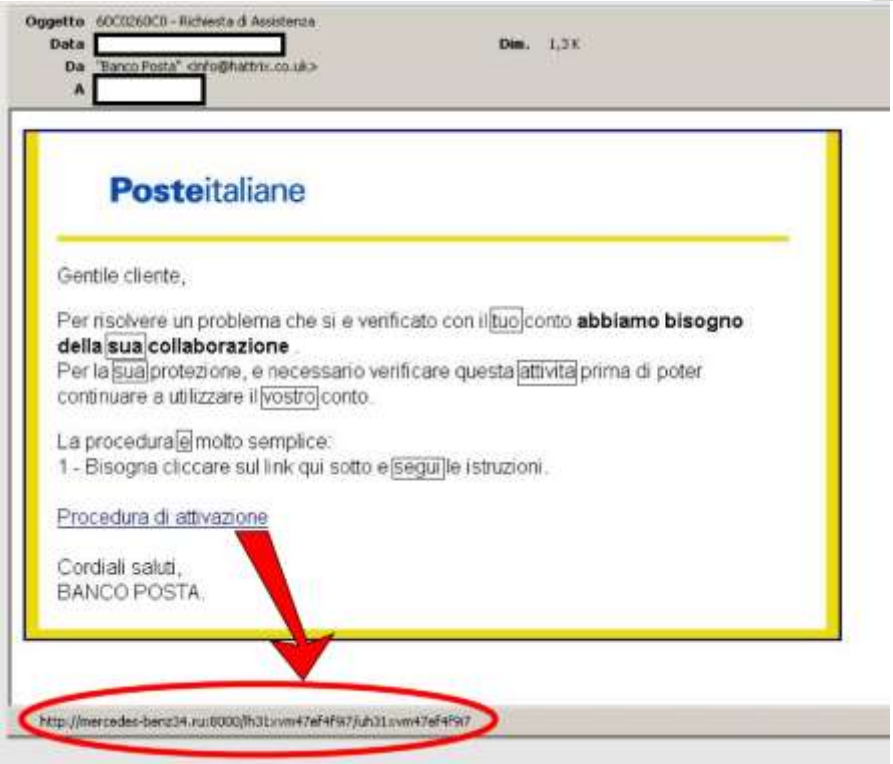
Lo spamming è l'invio di email ma anche messaggistica non voluta agli utenti. È un invio massivo di mail (spesso nell'ordine di migliaia di messaggi ed email) con l'intento di raggiungere il più alto numero possibile di utenti. Spesso i sistemi riceventi identificano correttamente i messaggi, come nell'esempio sotto. I messaggi finiscono in cartelle chiamate "spam" o "messaggi indesiderati" dove però è possibile ritrovarci anche messaggi leciti per errori negli algoritmi di filtraggio applicati. Non sempre lo spamming ha scopi fraudolenti e viene tipicamente usato per diffondere messaggi di marketing o pubblicità non desiderata.

Il phishing è un sistema di invio massivo di messaggi (spamming) e comunicazioni con l'intento specifico di recuperare credenziali, informazioni e metodi di pagamento dell'utente che, fidandosi, fa click su link che portano ad inserire tali informazioni su pagine web apparentemente legittime ma in realtà contraffatte.

Spesso, ma non sempre, all'interno del testo della mail sono presenti errori grammaticali e/o ortografici dovuti alle traduzioni automatiche da altre lingue, che ci possono allertare riguardo alla legittimità della comunicazione.

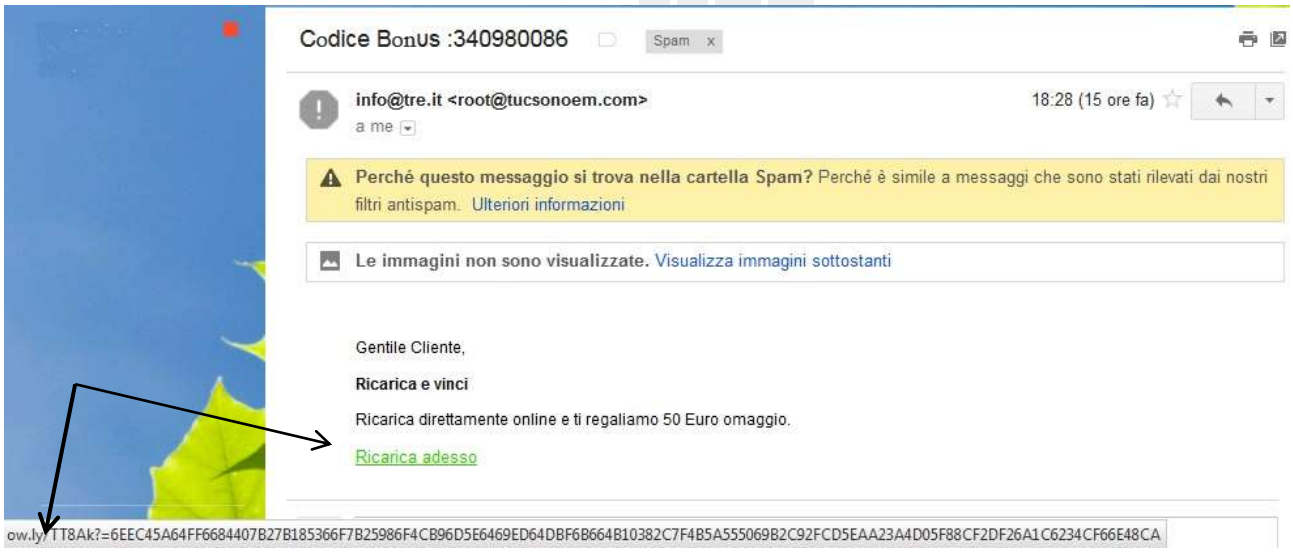
Qui sotto un esempio di messaggio di posta elettronica correttamente processato dal sistema come phishing.

Ma i messaggi diventano via via sempre più sofisticati e realistici e spesso è difficile riconoscere un'email di phishing da un'email legittima; nell'esempio qui sotto un messaggio di phishing che riesce ad eludere il sistema automatizzato di filtraggio.



Andando sopra il link (senza cliccare) nella barra di stato compare l'indirizzo del link che non ha nulla a che vedere con l'oggetto della comunicazione (nell'esempio Poste italiane).

Un altro esempio a seguire di mail non solo non voluta (spam), ma anche fraudolenta (phishing). Scorrendo con il mouse sul link "Ricarica adesso" si vede nella barra di stato in basso che l'indirizzo rimanda ad un sito sospetto.



Un sotto-insieme del phishing purtroppo in forte ascesa è il <u>pharming</u> che consiste letteralmente nell'instradare il traffico da un sito web legittimo verso un sito malevolo che apparirà come un sofisticato clone del sito originale.

1.2.5. Social engineering

In italiano viene detta ingegneria sociale e nel campo della sicurezza informatica, è lo studio del comportamento individuale di una persona al fine di carpire informazioni utili. Gli strumenti utilizzati nell'ingegneria sociale sono vari, inizialmente veniva utilizzato il telefono, attraverso il quale è possibile usare il linguaggio desiderato e l'approccio esatto per raggirare la vittima. Anche email e siti web vengono utilizzati nell'attacco, creando un contesto in cui le immagini e i messaggi possono portare il malintenzionato a ottenere dati riservati. Con la diffusione delle reti sociali negli ultimi anni, l'ingegneria sociale è tornata a svilupparsi, avvantaggiandosi anche di software (detti crawler) che analizzano le informazioni presenti in rete riguardo a specifici soggetti. Strumenti importanti sono anche la voce e il vocabolario utilizzato dell'ingegnere sociale, che attraverso lo studio del sistema da attaccare riesce ad adattarsi alla situazione in cui deve lavorare allo scopo di non destare sospetti. Le metodologie di attacco sfruttano principalmente tali tecnologie, avvantaggiandosi di tecniche psicologiche; vediamo alcune tecniche.

Viene creata una falsa ambientazione, o pretesto (pretexting), con lo scopo di spingere un utente a divulgare delle informazioni o a commettere azioni che non sarebbero consuete nel contesto in cui opera. L'attaccante si immedesima in una certa entità, sfruttando alcuni dati acquisiti in precedenza (data e luogo di nascita, codice fiscale, ecc.), per acquisire credibilità e fiducia da parte della vittima. In alcuni casi, l'attaccante può simulare il comportamento di una certa autorità importante come polizia o banca, spingendo la vittima a rispondere a tutte le domande che gli vengono poste senza esitazioni.

Il phishing è una tecnica per ottenere informazioni in maniera fraudolenta. Solitamente si invia una mail alla vittima, facendola assomigliare il più possibile ad un messaggio inviato da una certa compagnia o persona. La vittima viene spinta a scaricare un allegato che presenta un malware o a cliccare su un collegamento interno alla mail che porta ad una pagina web, molto simile a quella originale del fornitore del servizio, dove viene richiesto di fornire informazioni riservate come codice PIN bancario o password. Nell'ambito dell'ingegneria sociale è di uso frequente il phishing telefonico (vishing), nel quale viene simulato un contesto particolare come un contact center, attraverso il quale è possibile abbattere la diffidenza e ricevere maggiore fiducia da parte della persona coinvolta nell'attacco.

Altro mezzo diffuso è il baiting che consiste, nell'utilizzare un'esca per una persona in grado di accedere ad un determinato sistema (una sorta di cavallo di Troia). In pratica viene lasciato incustodito in un luogo pubblico (ingresso dell'azienda, parcheggio, bagno pubblico) un supporto di memorizzazione come una chiavetta USB, in modo da stimolare la curiosità della vittima che, con una certa probabilità, prenderà l'oggetto (facendo leva dunque su desiderio e avidità). In seguito lo strumento potrà essere utilizzato nel sistema nel quale lavora l'attore coinvolto, accedendo così molto più facilmente ai dati personali o aziendali essendo già all'interno della rete locale (LAN).

1.2.6. Ransomware

Un ransomware è un tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto (ransom in inglese) da pagare per rimuovere la limitazione. Ad esempio alcune forme di ransomware bloccano il sistema infettato e intimano l'utente a pagare per sbloccarlo, altri invece cifrano i file dell'utente, rendendoli inutilizzabili e chiedendo di pagare per riportare i file cifrati in chiaro.

I ransomware tipicamente si diffondono come i trojan, dei malware worm, penetrando nel sistema attraverso, ad esempio, un file scaricato o una vulnerabilità nel servizio di rete. Il software una volta attivato esegue una funzione (detta payload - dati utili effettivamente trasmessi), che ad esempio cripterà i file personali sull'hard disk del computer infettato, rendendoli così non più utilizzabili. I ransomware utilizzano spesso sistemi ibridi di criptazione sui documenti della vittima, adottando una chiave privata casuale e una chiave pubblica fissa. L'autore del malware è l'unico a conoscere la chiave di decrittazione privata. Alcuni ransomware eseguono un payload che non cripta i dati, ma è semplicemente un'applicazione che limita l'interazione col sistema, agendo sui file del sistema operativo o addirittura modificando il master boot record (MBR – le istruzioni di avvio del sistema) e/o la tabella di partizione impedendo l'avvio del sistema operativo finché non viene riparata.

I payload dei ransomware fanno anche uso di scareware (scare vuol dire "paura") per estorcere denaro all'utente del sistema impaurendolo attraverso finte minacce. Il payload a volte mostra notifiche o messaggi che, in modo molto credibile, potrebbero essere state inviate dalla polizia, le quali affermano falsamente che il sistema sia stato usato per attività illegali o che contenga materiale illegale, pornografico o piratato. Altri payload imitano le notifiche di attivazione prodotto di Windows, affermando che il computer potrebbe montare una distribuzione di Windows contraffatta, che va quindi riattivata. Queste tattiche forzano l'utente a pagare l'autore del malware per rimuovere il ransomware, sia con un programma che decritti i file criptati, sia con un codice di sblocco che elimini le modifiche fatte dal ransomware. Questi pagamenti di solito vengono effettuati tramite bonifico, con sottoscrizione via SMS, con un pagamento online, o, più recentemente, tramite Bitcoin (una criptovaluta digitale).

I ransomware più comuni che hanno colpito un maggior numero di vittime degli ultimi anni sono:

- Cryptolocker (2013): generava una coppia di chiavi RSA a 2048 bit e criptava i file. Il malware minacciava poi di cancellare la chiave privata se entro tre giorni dall'infezione non fosse stato versato un pagamento tramite Bitcoin. Si stima che il malware abbia estorto almeno 3 milioni di dollari.
- Wannacry (2017): il ransomware ha infettato oltre 230 000 computer in 150 paesi, con richieste di riscatto in Bitcoin in 28 lingue differenti. Europol lo ha definito come il più grande attacco ransomware di sempre e non si è diffuso tramite email come i precedenti, ma ha sfruttato una vulnerabilità di Windows.

1.2.7. Attacchi tipo brute force

Il metodo brute force (forza bruta), nella sicurezza informatica, indica una modalità di approccio per la risoluzione di un problema dato (ad esempio trovare una password) che consiste nel verificare tutte le soluzioni teoricamente possibili fino a che si trova quella effettivamente corretta. A fronte di essere una soluzione lenta e dispendiosa in termini di risorse di sistema, in linea teorica consente di trovare sempre la soluzione corretta.

Nell'ambito della sicurezza informatica, questo metodo si utilizza soprattutto per trovare la password di accesso a un sistema. La differenza principale tra attaccare una chiave crittografica e attaccare una password è che la prima è solitamente stata generata in modo totalmente casuale mentre una password, per la sua stessa natura di dover essere ricordata e inserita da esseri umani, è generalmente molto meno complessa. Anche il numero di caratteri dai quali è composta una password e la loro tipologia, determina il numero di combinazioni possibili che il sistema informatico che genera l'attacco brute force deve tentare.

Number of combinations

Category	amount	cumul.	6 charcters	8 characters
a - z	26	26	308.915.776	208.827.064.576
A - Z	26	52	19.770.609.664	53.459.728.531.456
0 - 9	10	62	56.800.235.584	218.340.105.584.896
&/$!	32	94	689.869.781.056	6.095.689.385.410.820

Quando sul sistema è possibile un attacco offline, ovvero quando l'attacco si può eseguire su una copia di lavoro locale del sistema da attaccare, si può compensare la lentezza di esecuzione con la quantità di risorse destinate all'attacco; laddove un singolo computer possa "provare" oltre 100.000 chiavi al secondo, due computer possono provarne il doppio e così via (la velocità aumenta linearmente con le risorse utilizzate). Questa caratteristica ha motivato, nei recenti anni, molti attacchi "distribuiti" sfruttando i cicli di lavoro inutilizzati di migliaia e migliaia di comuni computer (Internet facilita molto l'organizzazione di questo tipo di attacchi).

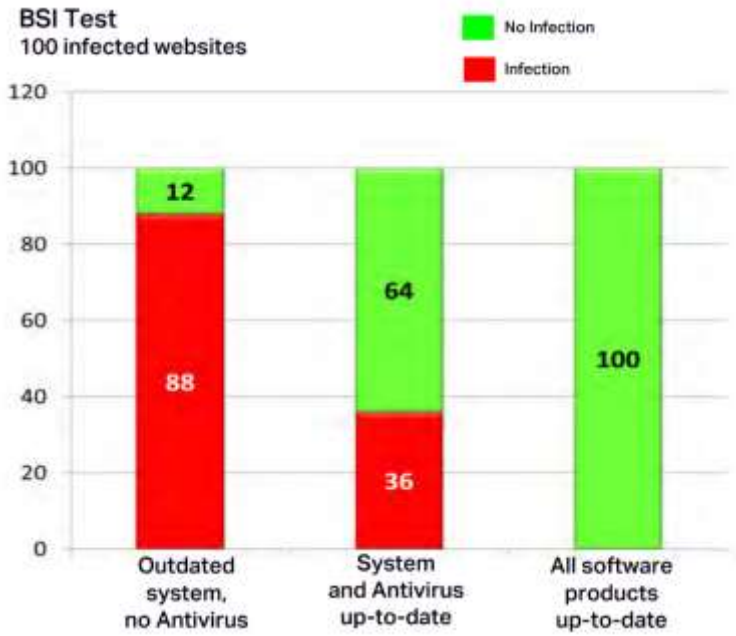
Gli attacchi brute force sono facilitati dalla leggerezza che la quale molti utenti generano le proprie password, riportando date di nascita, nomi comuni, sequenze scontate (es. elenchi di numeri successivi) e non le cambiano mai. Spesso le medesime password vengono utilizzate per più account su servizi diversi (es. email, home banking, social networks) e altrettanto spesso, milioni di record di utenze (id + password) vengono sottratti illegalmente dai server dei servizi on line (es. social network, email server, ecc.) e messi in vendita sul dark web (l'insieme dei siti e dei servizi internet raggiungibili solo attraverso reti private, nascoste e non rilevabili dai motori di ricerca). Questa combinazione rende gli attacchi brute force ancora attuali e redditizi per i cybercriminali.

1.2.8. Vulnerabilità dei software

I software che utilizziamo correntemente necessitano di un continuo aggiornamento sia per migliorarne il funzionamento sia per ovviare a possibili intrusioni esterne che sfruttano vulnerabilità presenti nei software stessi. Le vulnerabilità dei software potrebbero permettere ad esempio di intercettare i tasti premuti durante l'interazione con un programma o addirittura con il sistema operativo stesso e quindi con pagine web contenenti informazioni sensibili e informazioni di pagamento.

Andando per ordine di importanza fra i software al primo posto troviamo i sistemi operativi (OS) che vanno sempre mantenuti aggiornati appena si rendono disponibili aggiornamenti per la sicurezza (patch) dell'OS stesso. Gli altri aggiornamenti che vengono definiti secondari o addirittura facoltativi apportano miglioramenti a parti dell'OS ma non risultano così nevralgici come i precedenti.

I browser e i client di posta elettronica vanno costantemente aggiornati anche a rischio di perdere alcune funzionalità quando questi programmi interagiscono con altri software. Spesso i software ad alta rilevanza gerarchica come appunto i browser o client di posta agiscono in modo indipendente rispetto ad esempio ai plugin (piccole porzioni di software che permettono ulteriori funzionalità – esempio plugin per visualizzare i PDF all'interno del browser). Nuove versioni di questi programmi possono rinunciare, bloccandoli, all'utilizzo di quei plugin che vengono considerati poco sicuri o, ragione di più, pericolosi.



Risulta evidente, anche da test effettuati da aziende specializzate, che, mantenendo aggiornati tutti i software presenti sui device utilizzati (non solo computer ma anche smartphone, tablet, ecc.) si riducono drasticamente le possibilità di rimanere vittima di virus informatici.

Il cryptolocker Wannacry è stato lanciato nell'aprile 2017 grazie ad un exploit (programma informatico) che sfruttava una vulnerabilità dei sistemi operativi Windows obsoleti, ma già corretta da Microsoft con un aggiornamento di marzo 2017. Da una ricerca di ESET (produttore europeo di antivirus) emerge che nel Q1 2020 ancora il 40% circa degli attacchi ransomware segnalati era dovuto a questo cryptolocker ed alle medesime vulnerabilità di Windows del 2017. Questo significa che tantissimi device vengono infettati da virus, malware e cryptolocker soltanto perché non vengono aggiornati i SO.

2. Minacce e rischi legati alla Cybersecurity

2.1. I rischi che le persone corrono on line

I rischi che le persone corrono online sono molteplici e di varia intensità e/o pericolosità e possono includere crimini contro la persona e il patrimonio. Tra questi, piuttosto ricorrenti sono le molestie e il furto d'identità: quest'ultimo può essere utilizzato sia per arrecare danno diretto, che per mettere in atto comportamenti fraudolenti per interposta persona.

Tipicamente on line vengono commessi reati che rappresentano la versione digitale di reati già conosciuti che avvengono nel contesto fisico reale; ad esempio il cyberbullismo è la versione on line del bullismo. Tuttavia, visto il sempre maggior utilizzo di internet in tutti gli aspetti della vita, incluso quelli sociali, sono nati dei reati propri degli ambienti on line.

In questo capitolo andremo a conoscere i rischi collegati sia ai più frequenti reati che vengono realizzati via web a danno delle persone, sia ad insane abitudini nell'utilizzo degli strumenti on line quali, ad esempio, i social network:

- cyberbullismo
- revenge porn
- pedopornografia
- hating e cyberstalking
- sexting
- sextortion
- furto d'identità e di credenziali
- adescamento
- furto dei dati della carta di pagamento e/o del conto on line
- dipendenza dai social.

2.1.1. Cyberbullismo

Il cyberbullismo presenta le stesse caratteristiche del bullismo tradizionale, ma aggiunge degli aspetti che rendono il reato ancora più insidioso e persecutorio:

- il molestatore può risultare anonimo,
- è molto più difficile individuare la fonte dell'atto persecutorio,
- il molestatore può sentirsi eticamente alleggerito per il fatto, ad esempio, di non agire fisicamente contro la vittima e, in alcuni casi, può anche non rendersi pienamente conto di perpetrare un reato,
- vengono meno i limiti spazio-temporali: potenzialmente il cyberbullismo può investire la vittima ogni volta che questa si collega al mezzo elettronico usato dal cyberbullo (WhatsApp, Facebook, Twitter, etc.)

A differenza del bullismo tradizionale, il cyberbullismo può avvenire in qualsiasi luogo e a qualsiasi ora, in ragione dei mezzi e degli strumenti utilizzati (forum, social, email e quant'altro). La vittima può essere spinta a condividere contenuti con una persona che ritiene amica e che, invece, pubblica o diffonde ad un gruppo le informazioni ricevute: per i propri scopi il cyberbullo può anche creare contenuti ex novo o falsificarne altri già in suo possesso.

Una simile pressione può innescare un'angoscia persistente nella vittima che non riesce più a trovare luoghi e tempi per potersi difendere e sentirsi al sicuro. La vittima può, così, arrivare a sentirsi intrappolata e a non avere il coraggio di reagire, temendo un ulteriore inasprimento dell'offensiva del cyberbullo in caso di reazione. La situazione potrebbe complicarsi ulteriormente in presenza di minori, nei quali potrebbe essere presente anche la paura di una reazione negativa nei loro confronti da parte dei genitori.

Nei casi più estremi la vittima potrebbe ricorrere al suicidio ed è proprio per questo che occorre essere molto sensibili al problema e agire adottando tutte le contromisure possibili. Particolare attenzione va posta nel tipo di comunicazione che si stabilisce con chi ha subito l'offensiva, evitando di cadere in frasi ed atteggiamenti colpevolizzanti.

È consigliabile anche monitorare le reazioni intraprese dalla vittima sui social, dove una platea potenzialmente infinita potrebbe fare da cassa di risonanza a una recrudescenza dei toni e delle azioni, aumentando ulteriormente le pressioni sulla vittima. In alcuni casi il cyberbullo non è in grado di realmente quantificare il danno provocato alla vittima, cosa che rende ancora più pericolose le sue azioni. È quindi necessario bloccare quanto prima il cyberbullo sui social, parlarne con i genitori (in caso di minori) e ricorrere alle forze di polizia.

Il cyberbullismo costituisce una violazione del codice penale e civile ed è perseguibile dalle autorità competenti, come magistratura e forze di polizia.

2.1.2. Revenge porn, pedopornografia

In italiano revenge porn equivale a "vendetta pornografica". Si tratta di un reato che si compie diffondendo sui social immagini o video intimi di una persona a sua insaputa, con l'intenzione di compiere una vera e propria vendetta nei suoi confronti. Tipicamente alla base del desiderio di vendetta ci sono motivazioni di poco conto rispetto al danno arrecato, come, ad esempio, la fine di una relazione sentimentale.

Le immagini e i video possono essere stati ripresi nel passato da un partner e con il consenso della persona stessa, ma vengono in seguito utilizzati senza autorizzazione e per distruggere l'immagine di quella che diventa una vera e propria vittima. Il materiale utilizzato può anche essere estorto con forza e brutalità, ma, in ogni caso, sarà utilizzato e diffuso per causare il maggior danno possibile.

L'impatto sulla vittima può essere devastante, tanto che in Italia esiste una legislazione specifica, introdotta nel 2019, che tutela le vittime di violenza domestica e di genere, introducendo una corsia veloce e preferenziale per le denunce e le indagini riguardanti casi di violenza contro donne o minori.

Si configura come pedopornografia la rappresentazione di atti sessuali in cui siano coinvolti soggetti in età prepuberale. Non è da confondere con la pornografia minorile che, invece, coinvolge individui minorenni che abbiano già superato la fase puberale. Nella legislazione italiana è reato detenere, produrre, distribuire e pubblicizzare immagini e video che ritraggono bambini, bambine e adolescenti coinvolti in comportamenti sessualmente espliciti, reali o simulati (ad esempio, immagini realistiche o anche esito di manipolazioni grafiche) e qualsiasi rappresentazione degli organi sessuali di persone minorenni a fini sessuali.

Il continuo aumento di reati pedopornografici sembra essere legato anche ai seguenti fattori:

- l'aumento della fruizione di ambienti online da parte di bambini, bambine e adolescenti;
- l'aumento di contenuti sessuali autoprodotti e scambiati, in modo consensuale tra ragazzi/e, ma di cui, una volta messi on line, si perde il controllo.

Questo crimine è molto diffuso nel mondo web non indicizzato dai motori di ricerca ed è prevalentemente reperibile in canali di diffusione alternativi come il dark web - o web "oscuro" -, una sorta di "internet sommersa".

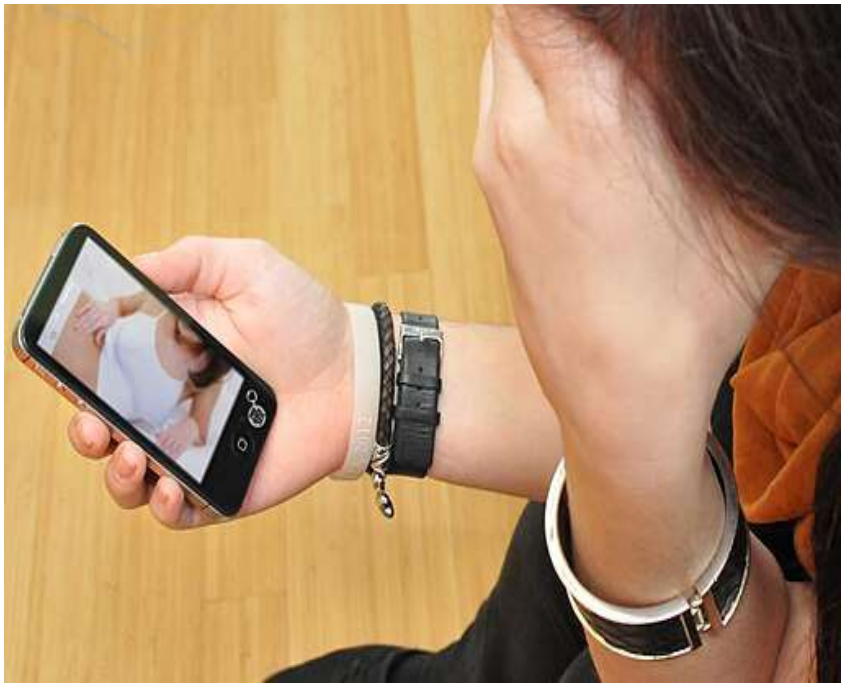
Nel rapporto annuale di INHOPE (https://www.inhope.org/EN/the-facts) 2020 - il network internazionale di 46 hotlines (piattaforme attraverso le quali è possibile segnalare materiale pedopornografico online) - oltre 250.000 immagini e video sono risultati illegali. Il 77% del CSAM (Child Sexual Abuse Material) coinvolge bambini e bambine al di sotto dei 13 anni; il 93% delle vittime è costituito da bambine e ragazze.

2.1.3. Grooming o adescamento on line

L'adescamento è un reato che parte da un adulto che tenta di avvicinare un bambino o un adolescente (inferiore ai sedici anni d'età) per scopi sessuali. Il reato si perpetua con qualsiasi atto volto a carpire la fiducia del minore attraverso artifici, lusinghe o minacce posti in essere anche mediante Internet. In particolare gli adescatori utilizzano, mascherando la propria identità, i servizi di rete tipo chat, blog, forum e social network per entrare in contatto con le vittime, conquistarne la fiducia e superarne le resistenze con il fine ultimo di avviare una relazione sessuale che concretizzarsi sia on line (via webcam) o anche dal vivo.

2.1.4. Sexting

Il termine deriva dall'unione di sex (sesso) e texting (inviare sms) e rappresenta la spedizione, ricezione e condivisione di testi, immagini o video che riguardano la sfera sessuale delle persone. Con l'evoluzione della tecnologia, il fenomeno nato con sms e mms (messaggistica tipica delle reti cellulari) si sta spostando ed estendendo sempre di più all'interno di social network, siti e blog, e lo scambio più spesso viene effettuato tramite bluetooth, email, chat e simili.



Ragazzi e ragazze spesso inviano immagini o video di sé stessi nudi o in pose ed atteggiamenti sessualmente espliciti a qualcuno di cui si fidano, esempio amici o partner. Il materiale scambiato resta disponibile on line e, anche dopo molto tempo, può essere divulgato senza consenso piuttosto che utilizzato, dalle stesse persone che prima erano amici o partner, per reati di revenge porn o sextortion.

2.1.5. Sextortion

SI tratta di una pratica illegale per estorcere denaro alle vittime. La tecnica è abbastanza semplice (ma evidentemente efficace): la vittima viene contattata attraverso un social network (es. Facebook) o un instant messanger (es. WhatsApp) da una persona che crea un profilo falso con foto di donne o uomini avvenenti: si tratta di esche sessuali. Dopo che tra l'adescatore e la vittima è nato un rapporto confidenziale, la conversazione si sposta su una qualsiasi videochat.

L'esca (spesso una donna) si spoglia e chiede al suo interlocutore di fare lo stesso davanti alla webcam, per ottenere foto e video osé. A questo punto − raggiunto lo scopo − la scena cambia: la donna sparisce ed al suo posto compare una richiesta di riscatto che solitamente viene rinforzata con la minaccia di pubblicare le immagini compromettenti sui social network alla lista dei contatti della vittima.

Le vittime vengono scelte in base alla loro situazione familiare e alla carica che ricoprono (per esempio un uomo sposato con figli o un professionista sono tra le vittime preferite). Questo persone hanno una maggiore probabilità di pagare il riscatto senza denunciare l'accaduto per nascondere le foto e i video. Infatti, secondo i dati della Polizia, solo una minima parte delle vittime presenta denuncia.

2.1.6. Cyberstalking

È la versione online del reato di stalking: con cyberstalking si indicano comportamenti molesti e persecutori attuati attraverso i nuovi mezzi di comunicazione (e-mail; messaggistica istantanea; social network; etc.).

Il cyber stalker approfitta dell'ampliamento della platea di utenti offerto dal web per tormentare e denigrare la vittima pubblicamente. L'obbiettivo è quello di indurre uno stato di costante ansia e paura in quest'ultima. Offese, minacce, insulti, ricatti, etc., possono minare seriamente il benessere psicologico della vittima perché, sebbene il cyber stalker esista "solo" virtualmente, le ripercussioni sono reali e tangibili. Si è visto che i persecutori possono essere sia uomini che donne, di qualsiasi età ed estrazione sociale.

Nel caso in cui ci si renda conto che una relazione, ancorché virtuale, stia minando la qualità della vita, è bene interrompere immediatamente ogni comunicazione, senza vergognarsi di chiedere aiuto.

2.1.7. Hating

Il fenomeno dell'hating deriva dall' hate speech (discorso d'odio) con cui oggi indichiamo una tipologia di comunicazione mirata a diffondere odio e pregiudizi. Con la diffusione del web e dei social network il fenomeno dell'hating si è esteso anche online dove produce una trasmissione su larga scala, tanto da arrivare a formare, a volte anche quasi involontariamente, delle community internazionali di haters che si raccolgono attorno all'odio condiviso provato nei confronti delle stesse persone/gruppi/comunità.

Un fenomeno che si è particolarmente sviluppato sulle piattaforme digitali, dove essendo maggiore la visibilità dell'utente, maggiore è anche l'esposizione al rischio. Commenti e risposte accanite ed offensive, a volte, si moltiplicano sui profili personali degli utenti; protetti dalla distanza virtuale che il social network riservano si arriva a scrivere cose che non si direbbero mai in faccia alle persone. Esistono, ad esempio, su Facebook gruppi che sono nati con l'intento di riunire persone accomunate dagli stessi interessi musicali, e allo scopo, quindi, di aggiornarsi su eventi e organizzarsi per concerti, e scambiarsi commenti e opinioni, trasformati di fatto in siti dedicati all'insulto contro i cantanti e gli stessi utenti.

L'hating online è quindi visibile sui profili di persone più o meno pubbliche, ma anche su pagine, blog e gruppi, dove nasce a tal proposito la figura del moderatore: una persona che si occupa di limare i contenuti nascondendo anche all'occorrenza i commenti troppo feroci o pericolosi. C'è chi sostiene però che questa sorta di censura possa ulteriormente fomentare gli animi più agitati e provocare effetti contrari.

Oggi il fenomeno risulta poco arginabile e la questione che vi ruota intorno è proprio quella dei confini tra censura e libertà di espressione.

2.1.8. Furto d'identità e credenziali

Il furto d'identità digitale è un reato che può comprendere diversi atti illeciti e che si articola nelle seguenti fasi:

- l'ottenimento delle informazioni personali della vittima,
- la gestione di tali informazioni, dal possesso alla vendita,
- l'utilizzo delle informazioni ottenute illecitamente per commettere ulteriori reati, contro il patrimonio (es. truffe, estorsioni) o contro la persona (es. diffamazioni o minacce).

Pur costituendo reato, nel Codice penale vigente il furto d'identità non è trattato da una norma specifica, ma è identificabile nei reati di sostituzione di persona (art. 494 c.p.) e di frode informatica (art. 640ter, comma 3, c.p.).

Sulla rete, cambiare o acquisire una nuova/altrui identità è estremamente facile: i numeri sulla diffusione sul furto d'identità digitale, riconducibili al fenomeno del cybercrime, sono in allarmante crescita. Tantopiù che è ormai dimostrata l'esistenza di vere e proprie associazioni a delinquere, che si dedicano al furto, alla vendita e allo scambio dei dati personali altrui illecitamente ottenuti.

Le più comuni frodi legate al furto di identità sono:

- clonazione dell'identità, ossia la sostituzione di una persona (in alcuni casi anche già defunta) con l'obiettivo di creare una nuova identità e una nuova vita;
- furto dell'identità allo scopo di utilizzare i dati identificativi di un individuo o di un'impresa per ottenere crediti, prestiti finanziari, aprire conti correnti, attivare carte di credito, in nome della vittima;
- impersonificazione in una persona diversa, tramite cellulari o servizi di social web, finalizzata al cyberbullismo con l'obiettivo di inviare messaggi e/o testi per vessare una vittima.

Tra le azioni che più frequentemente seguono un furto di identità c'è l'apertura di conti correnti bancari, la richiesta di rilascio di carte di credito, l'acquisto di beni, servizi e vantaggi finanziari. Azioni che di per sé non costituiscono un reato ma che sono realizzate a nome della vittima, utilizzando la sua identità, con l'obiettivo di trarne un illecito profitto economico. Le conseguenze per la vittima possono essere anche molto gravi, sia dal punto di vista finanziario che per il danno arrecato all'immagine.

In Italia, gli studi condotti dal CRIF - Centrale Rischi Finanziari - hanno dimostrato che il settore maggiormente colpito dalle frodi commesse con furto d'identità digitale è quello del credito al consumo. In pratica i cybercriminali effettuano acquisti di beni e servizi, tipicamente on line, pagandoli attraverso la richiesta di prestiti a nome delle loro vittime, delle quali hanno carpito le identità.

2.1.9. Carte di pagamento e conti on line

Cosa c'è di più prezioso dei propri dati personali e bancari? Entrare in possesso delle credenziali dei conti online, oppure dei codici della carta di credito di qualcuno, per riuscire a rubare direttamente dal conto corrente. Gli hacker cercano in tutti i modi di ottenerli in modo illecito tentando qualsiasi tipologia di attacco informatico, dal phishing (metodo sempre più utilizzato) al malware installato nel computer.

Il numero di attacchi informatici subiti dalle imprese e dai singoli cittadini cresce ogni anno di più e la crescita è dovuta alla facilità con cui gli hacker sviluppano virus e scoprono nuove modalità per infettare i dispositivi elettronici. Dall'altro lato, gli utenti spesso non sono in grado di riconoscere un attacco hacker e, spinti da abitudini d'uso non corrette ed imprudenti, cliccano sui link che arrivano tramite messaggio o email favorendo l'installazione di malware che consentiranno poi, al cybercriminale, di entrare all'interno del PC o dello smartphone e di carpirne i dati personali da utilizzare, o da rivendere nel dark web.

Secondo la Polizia Postale, sul mercato nero del dark web le informazioni complete di una carta di credito possono essere acquistate spendendo una cifra tra i 2 e i 6 euro. Un'identità completa, comprensiva di tutti i dati bancari, compresi quelli del conto corrente, costa poco meno di 20 euro. 500 euro, invece, è la cifra dovuta per ottenere i dati di un account PayPal. Per entrare all'interno di un PC, invece, bastano solo venti euro.

Per proteggere la propria carta di credito e l'accesso ai nostri conti on line, serve un po' di attenzione e di buon senso; alcuni accorgimenti per ridurre il rischio di cadere vittima di furti di danaro elettronico:

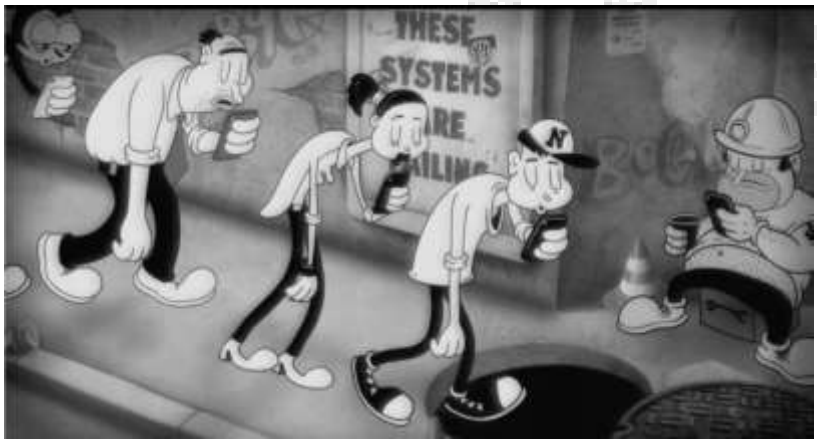
- in caso di acquisti on line verificare sempre con attenzione i certificati digitali, i livelli di sicurezza e di crittografia dei portali di e-commerce prima di inserire i dati della propria carta;
- preferire negozi on line conosciuti e diffidare delle promozioni con prezzi troppo bassi e non credibili;
- utilizzare carte di credito ricaricabili o virtuali usa e getta che, essendo valide sono fino ad un certo importo, consentono comunque di limitare il rischio;
- attivare, sia per i pagamenti con carta di credito on line sia per quelli con internet banking il sistema di autenticazione a più fattori che richieda di inserire codici di sicurezza inviati sullo smartphone e via email;
- evitare di inserire le proprie credenziali se ci si trova su una rete pubblica aperta (bar, aeroporto, ecc);
- se si riceve un'email proveniente (apparentemente) dalla vostra banca, nella quale vi si chiede di cliccare su un link e di cambiare password, prima contattate la banca, molto probabilmente si tratta di un tentativo di phishing.

2.1.10. Dipendenza da internet/social

Si tratta di un disturbo da dipendenza legato ad utilizzo intensivo e ossessivo di internet in tutte le sue forme e può riguardare diversi tipi di comportamenti disfunzionali messi in pratica on-line. Tra questi i principali sono: dipendenza da porno (sesso virtuale, pornografia, ecc.), gioco d'azzardo patologico, dipendenza dai social network (e, quindi, dalle relazioni virtuali), visualizzazione di filmati, videogiochi, shopping compulsivo, ricerca costante e ossessiva di nuove informazioni.

Non tutti coloro che utilizzano a lungo la rete corrono il rischio di sviluppare comportamenti di questo tipo, ed è più probabile che tale dipendenza si sviluppi in soggetti che presentino già disagi psicologici, come ansia e depressione, o che si trovino ad attraversare un momento particolarmente critico della propria vita (lutto, separazione, problemi economici/lavorativi). Particolarmente insidiosa è l'illusione di anonimato che la rete offre e che può portare i soggetti ad assumere false identità rischiando, alla lunga, di arrivare a un vero e proprio isolamento sociale che gli fa perdere i contatti con la realtà. I sintomi psico-fisiologici che possono derivarne sono mal di testa, tachicardia, disturbi alla vista, insonnia, confusione mentale, amnesia.

L'abuso dei social network e l'abitudine ad avere sempre con sé lo smartphone, non coinvolge soltanto i giovani, ma anche gli adulti che, secondo recenti studi, trascorrono in media 8-9 ore al giorno davanti a uno schermo. La dipendenza in alcuni casi può portare a trascurare studio e lavoro e a tralasciare attività basilari della vita, come mangiare e dormire. Il soggetto si trova a vivere in un mondo parallelo e irreale, dove tutto appare possibile e può trovarsi indotto a non percepire vincoli e limiti e a ritenersi libera di mettere in atto i comportamenti anche illeciti (es. bullismo, hating, pornografia, ecc.).



Strettamente legati ai meccanismi inconsci della dipendenza da internet e social sono i fenomeni di tolleranza/assuefazione (come il bisogno di aumentare il tempo in cui si sta connessi), astinenza (intenso disagio psico-fisico se non c'è possibilità di farne uso) e craving, cioè pensieri fissi e desiderio incontrollabile.

In particolare, per quel che riguarda l'astinenza, è da segnalare la cosiddetta sindrome da disconnessione: si verifica nei soggetti dipendenti quando non possono collegarsi ad internet (perché non c'è linea, hanno lasciato a casa lo smartphone, hanno la batteria scarica, ecc.) ed è caratterizzata da sintomi di ansia e panico e paura di rimanere soli. In casi simili è consigliabile ricorrere a un percorso di psicoterapia per aiutare il soggetto a riprendere in mano il controllo della propria vita.

2.2. Panoramica dei rischi da cybercrime per l'azienda

Così come le persone, anche le aziende corrono dei rischi specifici on line, considerando anche che per un'azienda la presenza su internet al giorno d'oggi è divenuta indispensabile. Sia che si tratti di un semplice sito aziendale cosiddetto "vetrina" (che ha la sola funzione di presentare l'azienda sul web e mostrarne l'offerta ed i contatti) o anche del solo utilizzo della posta elettronica, sia che si abbia a che fare con un'azienda completamente digitalizzata, che produce e/o vende solo via web, dovremo considerare attentamente implicazioni e rischi legati alla cybersecurity.

Infatti, a discapito del punto di vista di molti, il rischio di subire un cyberattacco non è correlato né alla grandezza dell'azienda, né alla sua ricchezza in termini di innovazioni, segreti tecnici o commerciali, disponibilità economico-finanziarie, numero o tipologia di clienti e/o dipendenti.

L'interesse dei cybercriminali è mosso quasi sempre dal fine economico e quindi la valutazione sull'obiettivo dei loro attacchi sarà spesso frutto di una semplice analisi costi/benefici. Tralasciando al momento le casistiche minoritarie legate a motivazioni politiche, di spionaggio e cyberguerra o all'attivismo, possiamo analizzare due diverse tipologie di attacchi finalizzati a procurare vantaggi economici illeciti:

- Cyberattacchi mirati, preparati con cura e realizzati da gruppi di hacker esperti che ricercano la modalità migliore per violare uno o più sistemi informatici di grandi aziende o enti per bloccarne l'operatività, rubare un qualcosa di interesse (es. dati personali o finanziari, segreti industriali, ecc.), prendere il controllo di un'infrastruttura (es. centrale elettrica) o chiedere un riscatto.
- Cyberattacchi su larga scala (phishing, ransomware, vulnerabilità software, social engineering, ecc.) realizzati utilizzando strumenti anche disponibili sul dark web (liste di utenti ed indirizzi rubati, malware pronti per l'uso in vendita, ecc). Si tratta di attacchi a basso costo, dove non si cerca di colpire una vittima specifica ma, lanciando un'esca su un gran numero di potenziali bersagli si aspetta che qualcuno caschi nella trappola. Non richiedono particolari competenze informatiche e sono in crescita esponenziale anno dopo anno.

Risulta evidente che, indipendentemente da quanto un'azienda è grande e ricca e da cosa produce o vende, tutte sono potenziali vittime degli attacchi del secondo tipo, i più diffusi. La domanda che ci si deve porre quindi non è se e come saremo attaccati, ma solo quando, e cosa succederà dopo. L' analisi del rischio informatico è il primo passo suggerito ad ogni azienda, piccola o grande, povera o ricca, analogica o digitale. Tale analisi, dovrà indicare a manager ed imprenditori le criticità più evidenti e le eventuali necessità di azioni, accorgimenti ed investimenti per la minimizzazione dei cyber rischi, per i quali, esistono peraltro anche coperture assicurative specifiche.

Fare impresa comporta la responsabilità di prendersi dei rischi che devono essere ben valutati, ponderati e gestiti nell'ambito dei diversi modelli di governance aziendale.

2.2.1. Data breach

Il data breach è una violazione dei dati nella quale è stato effettuato l'accesso o, peggio, la divulgazione in modo non autorizzato di dati personali, sensibili, riservati o comunque protetti.

Le violazioni dei dati possono verificarsi in organizzazioni di qualsiasi dimensione, dalle piccole imprese alle grandi aziende. Possono includere informazioni sanitarie personali, informazioni di identificazione personale (cd. dati personali), segreti commerciali o altre informazioni riservate.

Le più comuni esposizioni alla violazione dei dati includono informazioni personali, come indirizzi mail, telefonici, identificativi di account (id e psw), profili social, numeri di carta di credito, numeri di patente di guida e storie sanitarie, nonché informazioni aziendali, elenchi di clienti, progetti tecnologici e codice sorgente di software.

Se qualcuno che non è autorizzato a farlo visualizza i dati personali o li ruba, si dice che l'organizzazione incaricata di proteggere tali informazioni ha subito una violazione dei dati (data breach). Il data breach può riguardare anche informazioni su supporto cartaceo e non solo digitale.

Se la violazione dei dati comporta il furto di identità e/o una violazione dei mandati di conformità governativi o del settore di riferimento, l'organizzazione che ha subito il data breach può affrontare multe, contenziosi, perdita di reputazione e persino perdita del diritto di gestire l'attività. Anche il GDPR (Regolamento europeo per la protezione dei dati personali) disciplina le modalità di gestione in caso di data breach che coinvolga dati personali e indica le misure di sicurezza da attivare per evitarli.

Sebbene i tipi di violazione dei dati siano piuttosto vari, possono quasi sempre essere attribuiti a una vulnerabilità o scappatoia che i criminali informatici utilizzano per accedere ai sistemi o ai protocolli dell'organizzazione. Le potenziali cause di una violazione dei dati includono:

- credenziali di accesso deboli per qualsiasi applicativo o servizio web based,
- truffe di ingegneria sociale,
- malware o ransomware,
- phishing,
- hardware perso o rubato (computer portatili, dischi rigidi, dispositivi mobili),
- mancanza di controlli di accesso fisico agli ambienti aziendali,
- minacce interne (es. dipendenti infedeli),
- errori dell'utente; questa causa, detta fattore umano, è di gran lunga la più comune.

2.2.2. Failure data

Per failure data si intende una situazione in cui i dati non riescono ad essere recuperati a causa di un guasto hardware o software di un supporto o di un archivio di memorizzazione utilizzato (es. rottura di un hard disk o corruzione del firmare).

I guasti hardware e software sono le due principali cause di perdita di dati. Radiazioni di fondo, shock elettromagnetici, crash della testina e invecchiamento o usura del dispositivo di archiviazione rientrano nella prima categoria, mentre il guasto del software si verifica in genere a causa di bug (errori) nel codice stesso. Inoltre le fonti di errore oltre al sottosistema di archiviazione sul disco stesso possono essere molteplici; ad esempio, i cavi potrebbero essere leggermente allentati, l'alimentazione potrebbe essere inaffidabile, vibrazioni esterne come un suono forte, radiazioni cosmiche, ecc.

Da uno studio del CERN emerge che i bug del firmware hanno rappresentato il 5-10% dei guasti di archiviazione e che i tassi di errore osservati sulla corruzione silenziosa (errori che passano inosservati) sono pari a un bit ogni 4 GB (Gigabyte) di dati. Amazon.com ha riconosciuto tassi di corruzione dei dati simili nei loro sistemi. Si nota inoltre che mentre le capacità e la velocità dei dischi rigidi sono aumentate sostanzialmente, i loro tassi di errore sono rimasti invariati, il che significa che i dischi moderni non sono molto più sicuri dei vecchi dischi. Nei vecchi dischi la probabilità di danneggiamento dei dati era molto bassa perché memorizzavano piccole quantità di dati. Nei dischi moderni la probabilità è molto maggiore perché memorizzano molti più dati, pur non essendo sostanzialmente più sicuri.

Per evitare la perdita di dati a causa di guasti a supporti di memoria o applicazioni che li gestiscono o memorizzano, le soluzioni più comuni sono:

- Ridondanza dei dati, ottenibile con sistemi di memorizzazione RAID, per consentire ai sistemi di tollerare i guasti delle singole unità;
- Backup dei dati, per consentire il ripristino dei dati dopo un guasto fisico o la corruzione logica dei dati memorizzati.

<u>Recupero dati</u>

I dati di un'unità guasta a volte possono essere parzialmente o totalmente recuperati se il rivestimento magnetico dei piatti non viene completamente distrutto. Aziende specializzate effettuano il recupero dei dati, a costi significativi, utilizzando specifici strumenti software o aprendo le unità in una camera bianca (camera con qualità dell’aria controllata per evitare il deposito ad esempio della polvere o altre impurità presenti nell’atmosfera non controllata) e utilizzando l'attrezzatura appropriata per sostituire o riattivare i componenti guasti.

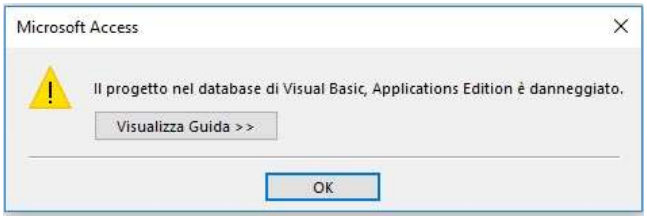
2.2.3. Data corruption

Per corruzione dei dati si intende il risultato degli errori che si possono verificare durante la scrittura, la lettura, l'archiviazione, la trasmissione o l'elaborazione dei dati stessi, e che introducono modifiche non desiderate agli originali. I sistemi informatici, sia essi hardware o software, di trasmissione e di archiviazione utilizzano una serie di misure per fornire l'integrità dei dati o l'assenza di errori.

Alcuni di questi errori, noti come corruzione silenziosa dei dati, passano inosservati, senza essere rilevati dal firmware del disco, dal sistema operativo che ospita il disco stesso o dai software di gestione dei database (archivi elettronici di dati).

In generale, quando si verifica il danneggiamento dei dati, un file contenente quei dati produrrà risultati imprevisti quando vi accederà dal sistema o dall'applicazione correlata. I risultati potrebbero variare da una piccola perdita di dati (output incompleto) a un arresto anomalo del sistema. Un esempio comune riguarda i file di documento: se danneggiati, quando una utente cerca di aprili con un'applicazione editor di documenti (es. MS Word o Openoffice) potrebbe ricevere un messaggio di errore, quindi il file potrebbe non essere aperto o anche aprirsi con alcuni dati danneggiati lasciando il documento incomprensibile).

Alcuni tipi di malware possono danneggiare intenzionalmente i file come parte dei loro payload, di solito sovrascrivendoli con codice non operativo o spazzatura, mentre un virus non dannoso può anche danneggiare involontariamente i file quando vi accede. Se un virus o un trojan con questo metodo di payload riesce ad alterare file critici per il funzionamento del software del sistema operativo o dell'hardware fisico del computer, l'intero sistema potrebbe essere reso inutilizzabile.



Alcuni programmi possono dare un suggerimento per riparare automaticamente il file (dopo l'errore) ed altri invece non possono ripararlo. Dipende dal livello di danneggiamento e dalla funzionalità integrata dell'applicazione per gestire l'errore.

Il danneggiamento dei dati può avvenire anche durante la trasmissione in rete per ha diverse cause come l'interruzione della trasmissione, interferenze di onde elettromagnetiche (es. forni a microonde) ed anche particolari condizioni metereologiche ed ambientali (soprattutto per le trasmissioni wireless).

2.2.4. Dati personali e sensibili

Sull'onda dell'evoluzione tecnologica e digitale degli ultimi anni il concetto stesso di dato personale è diventato qualcosa di più complesso rispetto a quello che intendevamo una volta. Oggi i dati personali sono tutte le informazioni che riconducono ad un singolo individuo attraverso le sue caratteristiche, relazioni, abitudini, stile di vita e così via.

I dati personali, secondo la definizione del GDPR (Regolamento UE 679/2016), sono:

- tutte le informazioni identificative, dai dati anagrafici alle immagini che ritraggono la persona;
- i dati precedentemente definiti sensibili e quindi sottoposti a tutela particolare;
- le informazioni giudiziarie che possono rivelare l'esistenza di determinati provvedimenti giudiziari a carico della persona;
- i dati relativi alle comunicazioni elettroniche via telefono o internet come, per esempio, un numero di telefono o un indirizzo IP;
- i dati che consentono di geolocalizzare una persona e da cui è possibile capire dove è andata, quando e a volte anche con chi;
- i dati genetici e i dati biometrici.

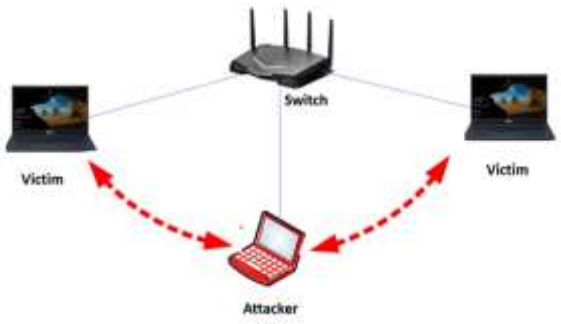
I dati sensibili venivano considerati dal Codice privacy (D.Lgs 196/2003) come quelle informazioni personali più delicate delle altre e che quindi dovevano essere trattate con estrema cura o non trattate affatto. Il codice considerava sensibili i dati personali in grado di rivelare ad esempio l'origine razziale ed etnica di un individuo, le sue convinzioni e adesioni religiose, politiche e filosofiche e lo stato di salute e la vita sessuale. Successivamente il GPDR definisce meglio quali sono:

- l'origine razziale o etnica,
- le opinioni politiche, le convinzioni religiose o filosofiche,
- l'appartenenza sindacale,
- i dati genetici e i dati biometrici intesi a identificare in modo univoco una persona fisica,
- i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Dati sensibili e dati particolari sono quindi assimilabili ed è vietato trattarli, a meno che l'interessato non abbia dato il suo esplicito consenso e salvo alcuni casi particolari previsti dalla normativa; in questo caso, vanno utilizzate particolari misure di sicurezza informatica ed organizzativa per il contenimento dei rischi di data breach, data failure e data corruption a tutela dei diritti e delle libertà degli interessati.

2.2.5. Truffe contro il patrimonio

Le truffe contro il patrimonio avvengono in ambito aziendale soprattutto attraverso la tecnica definita come man in the middle (uomo nel mezzo) che prevede che i cybercriminali riescano ad inserirsi, grazie all'accesso abusivo a caselle di posta elettronica ed altri account in uso alla vittima, in comunicazioni elettroniche che trattano di transazioni commerciali. L'obiettivo è quello di spiare il susseguirsi dei messaggi relativi alla transazione (fornitura, contratto, ecc.) allo scopo di sostituirsi ad uno dei due interlocutori e convincere la controparte ad effettuare il pagamento derivante dai propri obblighi contrattuali, su conti bancari diversi dai soliti, spesso collocati all'estero.



Secondo la Polizia Postale, si tratta di una truffa basata sulla 'fiducia' nelle fonti; il cliente si ritrova a ricevere la fattura (molto simile a quella vera) che attendeva dopo aver acquistato prodotti o servizi, con l'importo effettivamente speso ed inoltrata dal fornitore al quale si era rivolto. Tutto normale, all'apparenza. La vittima effettua il bonifico e paga la fattura, ma i soldi verranno accreditati sul conto del cybercriminale che intanto ha sostituito il codice IBAN dirottando i versamenti sui conti nella propria disponibilità, spesso registrati all'estero ed impossibili da confiscare.

Altra declinazione della truffa man in the middle in ambito aziendale è la sostituzione di persona: sempre attraverso l'accesso abusivo a caselle di posta elettronica delle vittime, i cybercriminali fanno pervenire agli uffici responsabili dei pagamenti, dei messaggi in arrivo dalle caselle di figure con alto livello di responsabilità in azienda. Questa mail, ovviamente false ed inviate all'insaputa dei mittenti ufficiali, richiedono di effettuare pagamenti su conti non conosciuti e dei quali vengono fornite le coordinate. Spesso gli importi non sono molto alti tanto che la vittima, che andrà poi ad effettuare il pagamento, non ritiene necessaria la richiesta di conferma alla mail che sembra realmente provenire dal vertice aziendale.

Le modalità operative descritte rendono obbiettivi perfetti le relazioni tra aziende dove spesso le informazioni e le disposizioni di pagamento vengono impartite on line. Alla base di queste truffe c'è la capacità dell'hacker di osservare e intercettare, o incanalare verso una cartella nascosta, sotto il suo diretto controllo, le mail provenienti dal soggetto interessato consentendogli, all'insaputa delle parti, di leggere, alterare o modificare il contenuto della corrispondenza per i suoi fini criminosi. Questa capacità deriva molto spesso da una non corretta gestione dei servizi di mail aziendale (es. uso da parte di più utenti diversi di indirizzi generici quali amministrazione@miazienda.it) o dall'uso di password non efficaci, non aggiornate ed uguali per più servizi.

2.2.6. GDPR

Il GDPR (General data protection regulation) è un regolamento dell'Unione europea in materia di trattamento dei dati personali e di privacy, adottato il 27 aprile 2016, che regolamenta il trattamento dei dati personali, ossia qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, anche se non registrati in una banca dati.

Da un lato vengono identificati i dati personali che includono dati identificativi come nomi, dati genetici, biometrici o inerenti alla salute, dati web come indirizzi IP, indirizzi e-mail personali, opinioni politiche e orientamento sessuale. I dati non personali, in contrapposizione, includono i numeri di registrazione della società, indirizzi di posta elettronica generici come info@azienda.com e dati resi anonimi.

Dall'altro lato vengono identificati coloro che forniscono e gestiscono i dati personali definendo tre termini principali:

- Con il termine "utente" si intende una persona i cui dati personali sono trattati.
- Con il termine "titolare del trattamento" si intende una qualsiasi persona fisica o giuridica coinvolta nella determinazione delle finalità e delle modalità del trattamento dei dati personali degli utenti.
- Con il termine "responsabile del trattamento" si intende una qualsiasi persona fisica o giuridica coinvolta nel trattamento dei dati personali degli utenti per conto del titolare del trattamento.

Il GDPR prevede che i dati possano essere trattati solo se sussiste almeno una base giuridica del trattamento. Al fine di effettuare un'attività di trattamento dei dati, l'organizzazione deve ottenere un consenso inequivocabile da parte degli utenti. In generale, al fine di ottenere il consenso al trattamento dei dati, le privacy policy devono essere redatte in modo leggibile, utilizzando un linguaggio e delle clausole comprensibili, in modo che gli utenti siano pienamente consapevoli di ciò a cui acconsentono e delle conseguenze del loro consenso.

Dal punto di vista di coloro che gestiranno i dati personali è prevista l'istituzione di un registro tenuto per iscritto "completo e esaustivo" delle particolari attività di trattamento dati che stanno svolgendo.

Viene inoltre istituito l'obbligo di creare un documento per iscritto denominato DPIA (Data Protection Impact Assesment) qualora l'attività di trattamento dei dati preveda un rischio elevato per i dati trattati degli utenti.

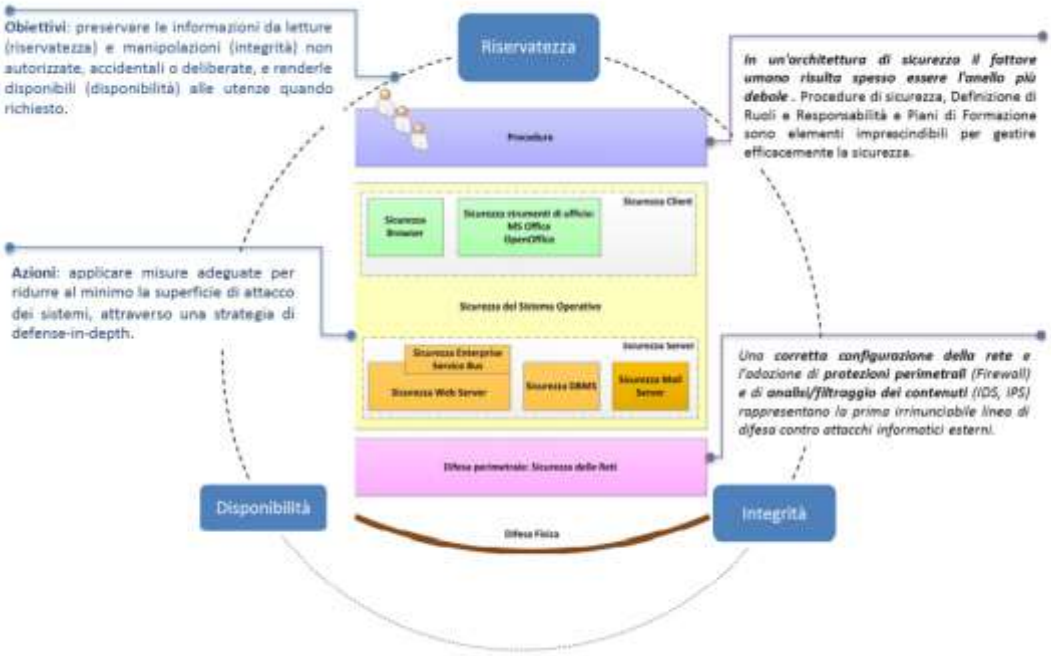
Le conseguenze per il mancato rispetto alle disposizioni del GDPR possono consistere in sanzioni pecuniarie di importo considerevole ed altri provvedimenti che possono essere attuati nei confronti delle organizzazioni che hanno commesso una violazione.

2.2.7. Linee guida AGID per la PA

La AGID (Agenzia per l'Italia digitale) ha emanato delle linee guida per la messa in sicurezza di una rete aziendale e delle infrastrutture informatiche della PA (Pubblica Amministrazione) che prevedono l'intervento dalle macro aree via via discendendo in modo granulare sino ad arrivare al singolo dispositivo PDL (postazione di lavoro).

In particolare sono previste specifiche indicazioni per:

- La gestione degli account (es. registrazione / cancellazione utenti, assegnazione/revoca di diritti, ecc.).
- La gestione dei fornitori per l'accesso alle informazioni o beni della PA e dei requisiti contrattuali sulla sicurezza per l'acquisto di beni e servizi.
- La gestione di regole e modalità di autenticazione degli utenti ai sistemi informativi, inclusa la separazione tra compiti e responsabilità e la protezione delle informazioni strumentali all'accesso (password management).
- La gestione degli eventi amministrativi di accounting e la registrazione degli eventi (audit) ed il monitoraggio degli accessi ai sistemi (log management).
- La strategia inerente alle procedure operative per la sicurezza all'interno della PA a partire dal back up fino ai test di vulnerabilità delle reti e le policy di aggiornamento dei software.
- La strategia della messa in sicurezza e l'omogenizzazione dei vari sistemi operativi in essere nella PA, a partire dalle regole per il loro aggiornamento fino ad arrivare alla sensibilizzazione del personale sui rischi che si corrono on line.



3. Buone pratiche per difendersi dal Cybercrime

3.1. Cosa fare in azienda

3.1.1. Gestione del rischio e difesa aziendale

Il cybercrime non è solo e soltanto un problema di tipo informatico o tecnologico e deve essere considerato uno degli aspetti della gestione del rischio.

La maggior parte delle aziende che nel mondo sono state colpite da NotPetya e WannaCry (due dei peggiori ransomware esistenti) si erano definite pronte contro le minacce cyber. Anche un'azienda che non è un obiettivo primario dei cyber attacchi lo potrebbe diventare per vie indirette come abbiamo visto nei capitoli precedenti. Nessuna azienda è quindi al sicuro su questo fronte senza uno specifico progetto che in modo trasparente consenta la gestione dei rischi in tempo reale ed in particolare si ponga l'obiettivo di:

- minimizzare il rischio che si possa essere oggetto di un attacco di cybercrime;
- attivare misure tecniche ed organizzative (strumenti, conoscenza, processi, tecnologia) per contenere al massimo i danni di un eventuale attacco;
- elaborare una strategia per gestire il rischio residuale in modo che un evento avverso non comprometta la continuità del business aziendale.

Le attuali migliori strategie per una corretta gestione dei rischi cyber prevedono:

- promuovere architetture IT semplici e, ove possibile, logicamente compartimentate, perseguendo un approccio Zero Trust, dove ogni accesso ai dati, interno o esterno, è ritenuto affidabile e deve quindi essere autorizzato.
- Attivare la protezione fisica e logica per la difesa del perimetro aziendale che ad oggi non è più solo un luogo fisico; un'azienda può anche subire un cyberattacco attraverso gli accessi ai sistemi IT di un dipendente in smart working.
- Affidarsi a fornitori specializzati per l'infrastruttura hardware/software ed i servizi di assistenza, manutenzione e sicurezza; condividere informazioni con i fornitori e delegare, anche formalmente, incarichi e responsabilità.
- Realizzare attività di formazione continua dei dipendenti per il corretto uso dei device aziendali e personali ed addestrarli a riconoscere le minacce.
- Investire per rendere sicuri i device ed i sistemi operativi aziendali (hardening), mantenendo aggiornato tutto il software ed attivando un piano di sostituzione degli apparati hardware obsoleti e vulnerabili.
- Realizzare un Piano di protezione e conservazione dei dati aziendali che, accanto alle policy di back up, definisca anche le modalità di test e di recovery.

3.1.2. Linee guida security per PMI

Il CIS (Cyber Intelligence and Information Security) dell'Università Sapienza in collaborazione col CINI (Consorzio Interuniversitario Nazionale per l'Informatica) ha elaborato, già dal 2019, il Framework Nazionale per la Cyber Security e la Data Protection.
https://www.cybersecurityframework.it/sites/default/files/framework2/Framework_nazionale_cybersecurity_data_protection.pdf . All'interno del documento trovano risalto i cosiddetti controlli essenziali che sono divisi in 8 tematiche principali:

1. Inventario, Asset Management – per sistemi, dispositivi, software, servizi ed applicazioni informatiche (anche di terze parti es. posta elettronica): sapere dove sono, il costo per il rinnovamento e il valore attuale, lo stato di aggiornamento in cui versano, stato della catena di backup, responsabili degli asset e della catena dell'informazione.
2. Governance: leggi e regolamenti ai quali prestare attenzione – GDPR regolamento UE 679/2016, ISO/IEC 27001:2013 lo standard internazionale sulla sicurezza delle informazioni, documenti emessi da ENISA l'agenzia europea per la sicurezza delle reti e dell'informazione.
3. Protezione dai malware – tutti i dispositivi che lo consentono devono essere dotati di sistemi antivirus ed antimalware regolarmente aggiornati.
4. Gestione delle password e degli account – complessità adeguata, cambio periodico, eventuale utilizzo di autenticazione a due fattori, cancellazione dei log di accesso, riservatezza delle password, account non utilizzati disattivati, accesso protetto (es. utilizzo VPN) fuori dal perimetro aziendale, accesso alle risorse strettamente necessarie.
5. Formazione e consapevolezza – Il personale deve essere sensibilizzato e formato sui rischi di cybersecurity e sulle migliori pratiche per l'impiego sicuro degli strumenti aziendali (es. riconoscere allegati e-mail, utilizzare solo software autorizzato, ...). Serve un piano di formazione aziendale dedicato a tutto il personale quantomeno per le nozioni basilari di sicurezza.
6. Protezione dei dati – progettare le difese informatiche avvalendosi di un consulente esperto, backup pianificati verificati e conservati in luogo sicuro.
7. Protezione delle reti – utilizzo di firewall e software anti-intrusione adeguati, dall'esterno della rete sistemi di VPN con conseguente criptazione del traffico.
8. Prevenzione e mitigazione dei danni – budget speso oltre che per i device anche per una corretta gestione del rischio, il miglior tecnico disponibile si troverà impotente di fronte all'ultimo malware o cryptolocker se l'organizzazione non avrà creato prima un piano di emergenza per problematiche non ancora scoperte e che di conseguenza non hanno ancora una soluzione.

3.1.3. Backup dei dati aziendale e politiche di conservazione dei dati

Il backup dei dati aziendali è uno degli aspetti cruciali di ogni strategia contro il cybercrime e le vulnerabilità hardware e software del proprio asset; inoltre garantisce la continuità del business dell'azienda in caso di eventi avversi per cause naturali (incendio o alluvione) oltre che per danni fisici all'infrastruttura (rotture e guasti).

Pensando a quanto si fa quotidianamente affidamento in azienda ai dati cruciali per la gestione del business: clienti, listini e prezzi, preventivi, ordini e dettagli di pagamento, ecc. Provando ad immaginare quanto tempo di si può andare avanti senza averne la disponibilità appare evidente che ogni tipo di business, indipendentemente dalle dimensioni, richiede un back up regolare dei dati importanti, essendo sicuri che tali dati siano i più recenti e che sia possibile ripristinarli.

In termini tecnici di parla di:

- il Recovery Time Objective (RTO): è il tempo massimo che si è disposti a trascorrere senza la disponibilità dei dati e definisce il modello operativo ed il tempo necessario al ripristino del sistema informativo aziendale.
- il Recovery Point Objective (RPO): è il momento più recente, indietro nel tempo, al quale si può tornare con il ripristino dei dati in caso di un problema e determina quindi la frequenza con la quale si dovrebbero fare i backup.

La strategia minima a cui fare riferimento può essere il modello backup 3 – 2 – 1:

3 diverse copie di tutti i dati necessari per il funzionamento dell'azienda; normalmente si tratta di documenti, foto, e-mail, contatti e calendari, database dei software utilizzati per la gestione del business, la maggior parte dei quali sono conservati in poche cartelle comuni sul computer, telefono o tablet o rete.

2 supporti differenti, ad esempio una unità NAS locale con l'aggiunta di un servizio cloud remoto (del quale è necessario conoscere bene i termini di servizio);

1 copia dei dati non raggiungibile dalla rete aziendale o dall'esterno, possibilmente off line anche se questo comporta un grosso impegno per tenerla aggiornata con le altre.

A questa strategia minima occorre affiancare l'ausilio di un fornitore specializzato dove il know-how aziendale non permette la gestione interna sicura e professionale dell'intera catena operativa del backup. Risulta fondamentale inoltre una verifica periodica dei backup ed un programma di test di ripristino.

I termini di conservazione dei dati sono determinati in parte dalla legge o da un contratto, mentre altri sono autodeterminati dal Titolare del trattamento. Un caso pratico per un'azienda potrebbe essere quello di decidere di conservare i dati relativi al rapporto lavorativo per un minimo di 10 anni. Scegliendo questa direzione è utile ricordare che gli obblighi di conservazione della documentazione fiscale è di 5 anni e quella relativa alla documentazione contrattuale è di 10 anni.

3.1.4. Proteggere l'organizzazione da virus, malware, ecc.

Per proteggere l'azienda nel modo più efficace contro virus e malware occorre diversificare e pianificare la strategia d'azione che, con le recenti evoluzioni sia delle tipologie di malware che delle tecnologie difensive, contempli la presenza congiunta di un firewall e di un antivirus/antimalware. Di cosa sono questi prodotti, che possono essere sia hardware che software, e di come funzionano abbiamo parlato nei primi capitoli di questa guida; vediamo adesso come si integrano relativamente alla protezione delle infrastrutture IT aziendali da virus e malware.

I moderni firewall sono diventati prodotti dinamici che integrano servizi sempre aggiornati e collegati al web e che sono in grado di fornire una barriera difensiva perimetrale alla rete attraverso una serie di funzionalità quali, ad esempio:

- Protezione antivirus a livello dell'intera rete bloccando i malware noti (virus, trojan, worm, spyware, ecc.) attraverso la scansione del traffico di rete sui principali protocolli.
- Anti Spam, un sistema di difesa per proteggere la posta elettronica dai malware.
- Filtro sugli accessi non voluti a siti web dannosi, compromessi o inappropriati.
- Intrusion prevention attraverso l'analisi approfondita dei pacchetti di dati in ingresso e uscita.
- Il monitoraggio delle applicazioni remote utilizzate via rete dal personale aziendale.
- La gestione di connessioni protette (VPN) per consentire accessi sicuri al personale che opera fuori dalla rete locale (es. Smart working).

I software antivirus sono invece deputati alla protezione degli endpoint, ossia tutti quei dispositivi in uso all'azienda capaci di connettersi alla rete (notebook, smartphone, stampanti, telecamere, ecc.) dal momento che le minacce del cybercrime (in particolare con i ransomware e altri malware) si sono dimostrate capaci di aggirare le classiche difese perimetrali.

Un software antivirus per l'Endpoint protection consente quindi di proteggere prodotti multipiattaforma (MS, Apple, Linux, Android, ecc.) attraverso una serie di tecnologie quali ad esempio la scansione della memoria degli apparati, il filtro per malware, il blocco degli exploit (ossia dei punti deboli o backdoors delle applicazioni), l'isolamento delle nuove minacce sconosciute fino al completamento dell'analisi di dannosità.

Un ulteriore livello di protezione riguarda gli account con cui le persone si collegano alla rete aziendale che richiederà una progettazione chiara, tesa ad evitare l'accumulo di autorizzazioni e privilegi eccessivi, oltre ad una gestione continuamente aggiornata. Gli account non più utilizzati dovranno essere periodicamente disattivati. Le singole utenze dovranno avere accesso alle sole cartelle di rete di pertinenza. Questo in caso di attacco permetterà una sorta di contenimento passivo (i virus non potrà accedere a tutte le cartelle di rete).

3.1.5. Mantenere sicuri smartphone e tablet

Nell'ambito dei sistemi operativi che vengono comunemente definiti "mobili", negli ultimi anni il mercato si è concentrato intorno a due principali prodotti:

- Android, è un sistema operativo Open Source basato su Linux che equipaggia gran parte (circa 85% nei primi mesi del 2021) dei dispositivi mobili (smartphone e tablet) dei principali produttori e che è distribuito da Google;
- iOS, sviluppato e distribuito da Apple è installato sui soli dispositivi Apple detiene una quota di mercato di poco più alta del 14%.

Entrambe le piattaforme possiedono una sezione e delle funzionalità sviluppate per poter gestire in modo efficace ed accentrato le risorse aziendali, tra le quali anche gli aspetti correlati alla sicurezza.

In particolare al link https://www.android.com/intl/it_it/enterprise/ si possono trovare informazioni ed istruzioni per l'utilizzo di Android Enterprise che consente di:

- ricercare il dispositivo migliore per le necessità aziendali,
- gestire, controllare ed aggiornare tutti i dispositivi a livello centralizzato,
- proteggere i dispositivi aziendali con più livelli di difesa,
- scaricare ed utilizzare applicazioni e servizi compatibili e certificati,
- consentire ai dipendenti di utilizzare i profili personali separatamente da quelli aziendali pur utilizzando un unico dispositivo.

Anche per Apple IOS, dal link https://business.apple.com/ si viene introdotti a Apple Business Manager, una soluzione di gestione che aiuta a configurare, proteggere e gestire i dispositivi, gli account delle persone ed i contenuti della propria organizzazione. Ad esempio, una soluzione di gestione consente di:

- visualizzare il proprio inventario di dispositivi,
- applicare criteri di sicurezza di base come il blocco schermo con un pass code e la crittografia dell'archiviazione,
- cancellare da remoto i dati se un dispositivo viene smarrito o rubato,
- distribuire e configurare app a livello centralizzato.

3.1.6. Policy di password management

La sottrazione delle password di accesso ai sistemi informativi (mail, gestionali, social network, ecc.) rappresenta il primo passo per un cyber attacco o un tentativo di frode on line. Le modalità per entrare in possesso in modo fraudolento delle password delle vittimo sono principalmente tre: facendosele dare dagli utenti (es. phishing, sniffing), comprando sul dark web quelle frutto di grandi data breach o attraverso un attacco brute force (software automatizzati che provano migliaia di possibili password fino a trovare quella giusta). All'interno dell'azienda devono quindi essere implementate delle policy di password management univoche che disciplinino la gestione delle singole password da parte di ciascun utente aziendale.

Le principali caratteristiche di un corretto password management sono:

- periodo massimo di durata della password (da 3 a 6 mesi massimo), dopo il quale deve essere cambiata senza utilizzare le ultime password precedenti;
- tempo minimo di durata della password per impedire ai più *creativi* di cambiare la password molte volte in pochi minuti, con l'obiettivo di fatto di riutilizzare la *medesima* password, eludendo il vincolo del punto precedente;
- la complessità minima delle password (almeno 8 caratteri con combinazione di caratteri maiuscoli, minuscoli, numeri e caratteri speciali);
- ove possibile implementare l'autenticazione a due fattori (es. fatta il login sul sistema informativo, arriva un codice di verifica sulla mail o via sms sul telefono abbinato con cui completare la procedura di autenticazione);
- disabilitazione degli gli account non più utilizzati;
- blocco dell'account dopo un certo numero di tentativi di inserimento password falliti;
- divieto di comunicare la propria password ad altri, nemmeno colleghi (nel caso dovesse essere indispensabile, procedere immediatamente dopo a modificarla);
- divieto di scrivere le proprie password su fogli o supporti accessibili ad altre persone;
- divieto di condivisione delle proprie password *in chiaro,* nemmeno sui propri device personali (es. inviare la password ad altri con un messaggio).

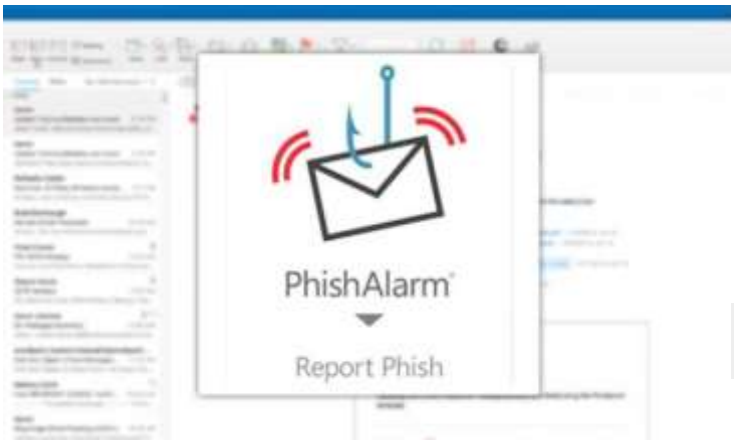
In aggiunta a queste policy, in caso di gestione di dati particolarmente critici, si potrebbero aumentare ulteriormente le difese applicando ai device fissi e mobili ulteriori livelli di sicurezza utilizzando ad esempio hardware ad autenticazione biometrica o smart card.

3.1.7. Proteggersi dal phishing e dal thief information

Per proteggere adeguatamente l'azienda dal phishing, dai malware e dal furto di informazioni in genere (thief information) è opportuno un approccio che tenga conto dei seguenti aspetti, in parte già trattati in questa Guida.

1. Tecnologico: prevedere l'utilizzo di strumenti tecnologici hardware e software che proteggano l'infrastruttura dell'azienda (es. firewall, antivirus, filtri email, software aggiornato ecc.) o che contribuiscano a garantirne la resilienza (es. back up, cloud, ecc.).
2. Organizzativo: definire, pubblicare e far rispettare le policy di utilizzo dei device aziendali o di password management, prevedere procedure per il test delle misure di sicurezza e del restore dei back up, riprogettare la rete aziendale.
3. Umano: considerare che il fattore umano, che resta spesso l'elemento più debole della catena di protezione aziendale, può trasformarsi in un importante barriera difensiva se opportunamente formato ed allenato.

Tralasciando uno solo di questi assetti si rischia di compromettere gli investimenti fatti sugli altri e, tipicamente, le aziende tendono a curare prima gli aspetti tecnologici, poi quelli organizzativi e solo in ultima istanza quelli umani. Viceversa la base di partenza dovrebbe sempre essere un'adeguata formazione del personale con specifiche campagne anti phishing: vedere e conoscere concreti e contestualizzati esempi di phishing permette alle persone di riconoscere i casi reali e mantenere sempre alta l'attenzione.



La formazione quindi dovrà essere continua e prevedere sia un livello minimo di competenza e consapevolezza da raggiungere subito, sia aggiornamenti, non solo in funzione dei trend tecnologici o delle sempre nuove modalità di attacco dei cybercriminali, ma soprattutto per allenare le persone ad essere vigili ed a reagire di fronte a situazioni inattese. Proteggere la propria organizzazione con le più moderne risorse hardware e software e sottovalutare il fattore umano porterà inevitabilmente a un fallimento, in particolare in presenza di lavoratori in Smart working. A casa le persone si sentono più sicure e protette ma non è così, anzi, spesso si è più esposti agli attacchi dei cybercriminali e si rischia anche di trasferire sulla rete aziendale malware residente sul computer di casa. Di contro spesso gli Smart worker sono più disponibili ad imparare e l'e-learning può essere il miglior bilanciamento tra costi e benefici in contesti aziendali. Anche per la formazione sulla cybersecurity è consigliato rivolgersi a fornitori specializzati che possono utilizzare specifici tool di formazione a distanza, come gaming e narrazione multidisciplinare.

3.1.8. Cosa fare se … il ruolo della Polizia postale

Nel caso si ritenga, o si abbia anche solo il dubbio di essere bersaglio o vittima di attacchi di cybercrime, la prima cosa da fare è interpellare immediatamente il proprio fornitore di servizi di assistenza informatica, valutando insieme la situazione. Il vostro specialista di fiducia, dopo aver analizzato la situazione e la minaccia, saprà consigliarvi al meglio per procedere a cambiare le password (anche a scopo cautelativo), a bloccare account o servizi di pagamento ed eventualmente a denunciare il fatto.

Se si è vittime di un reato informatico o anche solo di un tentativo di truffa è comunque sempre consigliato rivolgersi alla Polizia Postale, una speciale sezione della Polizia di Stato deputata alla prevenzione e contrasto ai crimini informatici e dotata di professionalità e strumenti adeguati. È possibile richiedere l'intervento del Commissariato di Pubblica sicurezza direttamente online (sul sito www.commissariatodips.it/ dove è possibile segnalare i tentativi di truffa o altri reati informatici direttamente da un form online) per far sì che siano raccolte tutte le informazioni necessarie per perseguire i crimini informatici.

All'interno del sito stesso si trovano anche approfondimenti e informazioni utili per contrastare il cyber crime.

Se poi ci si dovesse accorgere che il proprio account di posta, social network, messaggistica risulta compromesso, è bene avvisare i propri contatti del fatto che i messaggi in arrivo dai vostri indirizzi non sono più affidabili.

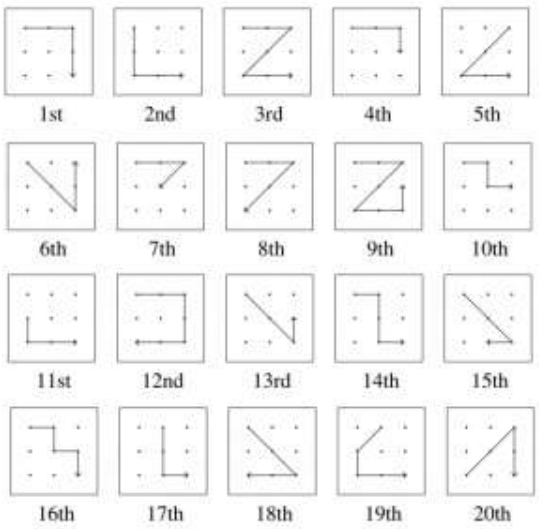
3.2. Cosa fare personalmente in più

3.2.1. Bloccare l'accesso ai propri dispositivi

La messa in sicurezza dei dispositivi personali con un sistema di riconoscimento valido è un requisito fondamentale per il loro utilizzo, per soli scopi privati o anche per uso professionale. Molte organizzazioni tra l'altro attuano la politica del BYOD (Bring your own device – Porta il tuo dispositivo) che prevede appunto l'utilizzo di dispositivi personali in contesti produttivi aziendali o scolastici.

Oggi una moltitudine di servizi viene ormai svolta su questi strumenti: messaggistica istantanea ed e-mail, social network, servizi di home banking, ecc.; in pratica una parte notevole se non quasi la totalità della nostra vita digitale transita da smartphone e notebook e vi lascia una traccia. Così come si chiude a chiave il portone di casa (a volte anche con doppie serrature di sicurezza), si installano antifurto e videocitofoni, i dispositivi elettronici attuali non possono e non devono essere utilizzati senza uno dei sistemi di sblocco presenti sul device stesso. Mentre su computer e notebook è comune l'uso di password o di sistemi di autenticazione forte quali smart card con certificati digitali (es. CIE - Carta di identità elettronica), sugli smartphone gli attuali sistemi di sblocco sono, in ordine di sicurezza decrescente:

- sblocco attraverso il volto in 3D, il migliore in quanto non può essere ingannato da una foto (2D);
- impronta digitale, occorre registrarne più di una, sia per praticità sia perché un piccolo taglietto o escoriazione può impedire il corretto riconoscimento;
- PIN a 6 cifre non banale (esempio 123456), in caso di fallimento dei precedenti o al riavvio del device può sbloccare il device;
- segno/sequenza di tracciamento con le dita: ci sono degli schemi piuttosto semplici per individuare i segni più utilizzati (esempio spirale o zigzag vari).



Per quanto riguarda lo sblocco tramite segno (fatto con lo scorrere del dito) su vari siti si trovano quelli più comunemente usati. È possibile ovviamente farne di più complessi ma spesso poi si opta per cambiare con un segno più veloce e qui i pattern (schemi) non sono poi così tanti.

Occorre quindi selezionare il sistema di blocco/sblocco che meglio si addice alle proprie caratteristiche (anche per la sua memorizzazione) e configurarlo, avendo cura di attivare anche le procedure per il recupero dei codici di sblocco (es. domanda segreta, numero di telefono o indirizzo email associato, ecc.). Infine non dimentichiamo di impostare il blocco automatico del dispositivo dopo un breve periodo di inutilizzo (in funzione delle proprie abitudini d'uso).

3.2.2. Backup dei dati personali

Come abbiamo visto per le aziende, anche per le singole persone il backup dei dati personali è uno strumento fondamentale e insostituibile per vari motivi. Un primo fondamentale motivo è il malfunzionamento del device; senza un backup valido e possibilmente recente rischieremo di perdere i contenuti del device stesso. Sia i principali vendor di smartphone (Samsung, Huawei, ecc.) che i distributori dei sistemi operativi Android (Google) e iOS (Apple) offrono sistemi di backup su altro supporto, che può essere il computer ma anche il cloud (di solito un piccolo spazio di archiviazione gratuito e più grande a pagamento). È importante quindi, volendo anche contenere i costi del back up, scegliere quali tipologia di contenuti e dati si ritengono più importanti (es. contatti, foto, registro delle password, preferiti e/o cronologia, del browser, ecc.) ed impostare il loro back up che dovrà avvenire preferibilmente in automatico (in modo da non doversene ogni volta ricordare).

Anche le app di messaggistica prevedono spesso un backup dei dati sul cloud, ad esempio WhatsApp si appoggia all'account Google per eseguire il backup delle chat ma con spazio gratuito limitato.

Ricapitolando possiamo avere uno schema come il seguente:

Backup	**servizio**	**facilità**	**costo**
Android	cloud	Molto facile	Gratuito per spazio limitato, altrimenti occorre acquistare spazio aggiuntivo su Google Play Store
iOS	cloud	Molto facile	Gratuito per spazio limitato, altrimenti occorre acquistare spazio aggiuntivo su Apple Store
Android	Su computer	Da facile a medio	Gratuito ma occorre copiare manualmente le cartelle e i files o affidarsi a programmi appositi (spesso il produttore del device ha una sua applicazione dedicata)
iOS	Su computer	Da facile a medio	Gratuito ma occorre utilizzare l'applicazione iTunes di Apple o una features di Mac OS
Singola app	Su cloud o su computer	Da facile a medio	Gratuito per spazio limitato nel cloud a cui si appoggia l'applicazione o se possiamo fare il backup su computer (copia/incolla). A pagamento se vogliamo più spazio nel cloud.

Il backup è importante anche in caso di violazione (accesso indesiderato) dello smartphone o di furto/smarrimento. Da remoto attraverso l'apposita funzionalità (che deve essere attivata in precedenza) trova il mio telefono (Google) o trova il mio iPhone (Apple) sarà possibile bloccare il device e cancellarne i dati che, grazie al backup in nostro possesso, potremo poi recuperare per installarli su un nuovo dispositivo.

Anche il computer personale ha bisogno del backup a salvaguardia di tutti i documenti che ci sono salvati, spesso si tratta di foto, filmati e documenti di una vita. Ad oggi, i sistemi operativi più diffusi (MS Windows, Mac OS) hanno specifiche funzionalità di backup automatico che occorre configurare per le proprie necessità, utilizzando supporti di memoria esterni o servizi cloud.

3.2.3. Gestione delle proprie password

Per la corretta gestione delle password di accesso ai vari siti e servizi on line oggi indispensabili (email, social network, home banking, ecc.) si può fare riferimento al precedente paragrafo dedicato al Password management: le regole e gli accorgimenti da usare sul posto di lavoro restano validi anche in contesti privati.

Vista il numero non trascurabile di password da gestire e la necessità di cambiarle con frequenza e di utilizzare le medesime per più servizi, si pone un importante quesito su dove conservare queste password.

Tipicamente, per i servizi fruibili via browser web, si può utilizzare la funzionalità di accesso automatico presente in tutti i principali browser (Chrome, Firefox, Safari, Edge, ecc.) che consente di memorizzare le credenziali nel portachiavi.

Affinché questa soluzione risulti sicura, è necessario avere sempre cura di accedere al proprio account sul browser, prima di memorizzarci le password (alla prima digitazione il browser richiederà in automatico di salvare le credenziali), e di proteggere tale account con l'autenticazione a due fattori già descritta in precedenza.

Anche i sistemi operativi dei dispositivi fissi o mobili hanno la funzione *portachiavi* e consentono il salvataggio delle credenziali in modalità segreta; anche in questo caso dobbiamo assicurarci che l'accesso ai dispositivi risulti protetto da password e da blocco, come descritto in precedenza.

Un valido aiuto può risultare un software di Password Management, ossia una app (ovviamente protetta da riconoscimento biometrico o da una password forte che sarà l'unica che poi ci dovremo sempre ricordare), all'interno della quale salvare tutte le altre password. Ce ne sono diversi disponibili on line, a pagamento o anche gratuiti (con licenza Open source) che funzionano sui principali sistemi operativi, fissi o mobili (es. Keeper, Bitwarden, LastPass, 1Password, RoboForm, KeePass, ecc.).

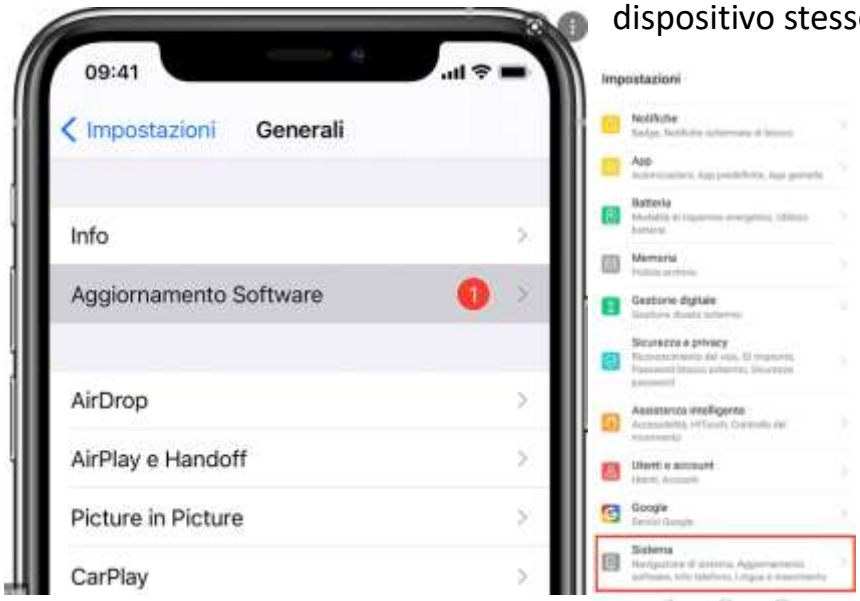
Si tratta di software sicuri che applicano protocolli di sicurezza elevati come la crittografia con chiavi a 256 bit generate casualmente, per proteggere le informazioni; inoltre la maggior parte dei gestori di password criptano localmente, il che significa che, prima che le vostre password vengano salvate nel password manager, queste vengono criptate in modo che nessuno venga a conoscenza di informazioni sensibili.

Alla prima apertura dell'applicazione è consigliato impostare un robusto PIN alfanumerico (fondamentale perché accedendo al database avremo disponibili tutte le nostre password) o l'impronta digitale. Sarà possibile successivamente sincronizzare il proprio database delle password tra vari device (smartphone, tablet, computer, ecc.) ad esempio collocando il database su uno spazio cloud (possibilmente criptato).

3.2.4. Aggiornamenti di sistema per la sicurezza dei dispositivi

Come abbiamo già visto in precedenza, il mancato aggiornamento dei software in generale e dei sistemi operativi in particolare rappresenta una importante vulnerabilità attraverso la quale i dispositivi possono essere attaccati dai malware. Aggiornare il sistema operativo del proprio device iOS, Android o Windows è di fondamentale importanza quando si parla di sicurezza informatica. Le patch di sicurezza dei sistemi operativi non sono mai facoltative, in quanto vanno a risolvere criticità o bug software che via via vengono scoperti. Si può eventualmente soprassedere per qualche tempo sui cosiddetti aggiornamenti facoltativi. Quando un produttore rilascia un aggiornamento di sistema per il proprio device è importante aggiornarlo quanto prima avendo a disposizione (nel caso si trattasse di un dispositivo portatile) di una buona percentuale di batteria disponibile o di un caricabatteria.

I sistemi operativi precedenti a Windows 10 non sono più soggetti ad aggiornamenti da parte di Microsoft e quindi risulta di capitale importanza provvedere all'aggiornamento a Windows 10 nel più breve tempo possibile, pena la vulnerabilità derivante da non avere patch di sicurezza aggiornate sul proprio sistema. Ugualmente, anche per i dispositivi mobili, è necessario aggiornare il sistema operativo all'ultima versione disponibile per le caratteristiche del dispositivo stesso.



Nel 2017 molti utenti nel mondo sono rimasti vittima dell'attacco ransomware WannaCry perché non avevano aggiornato il loro sistema operativo Microsoft Windows.

Se lo avessero fatto con regolarità, avrebbero beneficiato dell'importante patch di sicurezza rilasciata da Microsoft prima dell'attacco.

3.2.5. Difendersi dal phishing

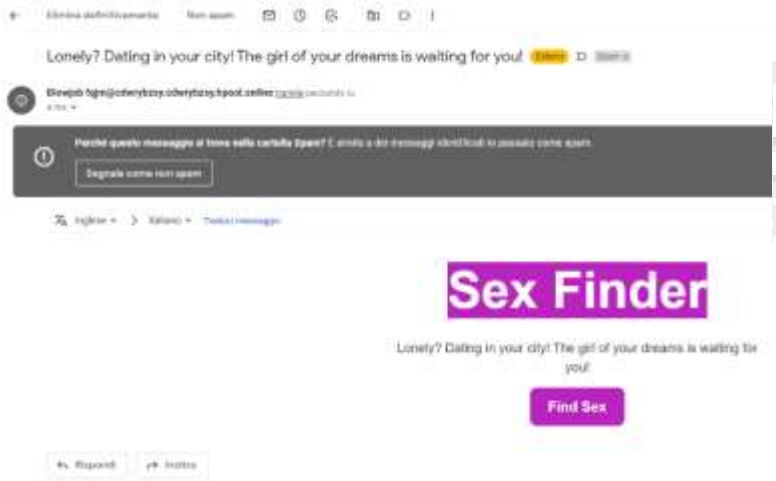
Abbiamo parlato in precedenza di come difendere un'organizzazione dai tentativi di phishing, adesso vedremo alcuni accorgimenti che possono essere messi in pratica per evitare di abboccare alle trappole dei cybercriminali. La migliore strategia per difendersi dal phishing è applicare alle proprie attività on line lo stesso buon senso e gli stessi scrupoli, che dovremmo applicare nella vita reale per non essere truffati.
Quando ci troviamo di fronte ad una mail, o ad un messaggio in genere (il phishing si diffonde anche attraverso i social network e le app di instant messaging), dovremo:

- Leggere con cura il messaggio (compreso il mittente e l'oggetto) che ci arriva; spesso sono presenti dei piccoli errori di grammatica o di ortografia che ci dovranno far insospettire.
- Copiare e incollare su una nuova finestra del browser il link presente nel messaggio ci darà ulteriori informazioni: diffidare di un link che non riporta al sito ufficiale del fornitore di servizi, con presente il protocollo di sicurezza https (e non http, non sicuro) evidenziato dal lucchetto chiuso (cliccabile per dettagli sui certificati di sicurezza) sulla sinistra della barra degli indirizzi.
- Piccoli errori di ortografia possono far apparire un URL identico a un sito legittimo, ad esempio, 0 (numero) e O (lettera), l (L minuscola) e I (i maiuscola), oppure vv (per w). È possibile copiare e incollare un URL in una barra di ricerca, se ci sono caratteri sostituiti o piccoli errori di ortografia nell'URL, la ricerca riconoscerà il trucco.
- Attenzione agli URL abbreviati; potete utilizzare servizi web affidabili, ad esempio https://www.phishtank.com/ per verificare il link stesso, copiandolo e incollandolo nell'apposito spazio.
- Mai cliccare su link numerici (ad esempio http://57.39.125.43) a meno di essere completamente sicuri della destinazione, ad esempio un URL legittimo interno alla propria azienda.

I messaggi di phishing utilizzano indirizzi email o siti web contraffatti per assomigliare a quelli legittimi di una organizzazione come la banca o l'emittente della carta di credito, un portale di pagamenti o di e-commerce, o anche un'organizzazione governativa. Di solito chiedono di aggiornare le nostre informazioni ed avvisano che in mancanza di un aggiornamento urgente ci saranno delle conseguenze spiacevoli (es. certi servizi saranno bloccati); a volte promettono ricompense o affari straordinari (es. acquisto di prodotti di moda a prezzi bassissimi) e cercano di dirigerci, attraverso un falso link, verso un sito contraffatto per carpire le ns credenziali; altre volte richiedono di scaricare ed aprire un allegato (es. fattura, ordine o altro documento) attraverso il quale installano un malware sul nostro dispositivo. La soluzione migliore è marcare come spam e cancellare subito la mail o il messaggio sospetto o, volendo approfondire, mettersi in contatto con il mittente attraverso un numero telefonico sicuro cercato sui canali ufficiali dell'organizzazione (non quello indicato nel messaggio sospetto). Nel dubbio di aver inserito eventuali credenziali su una pagina sicura, procedere immediatamente a modifica la password del servizio in questione.

3.2.6. Proteggere la propria casella email

La casella e-mail è il fulcro di gran parte della nostra attività online sia privata sia aziendale. Quasi tutti i servizi che utilizziamo fanno riferimento all'indirizzo mail principale e, in alcuni casi, ad uno secondario, sia come riferimento primario di un account (nome utente), sia in caso di problematiche di accesso (recupero password). Per questo motivo un indirizzo mail compromesso comporta una gravissima vulnerabilità nelle nostre attività. Risulta fondamentale proteggerlo in modo efficace cambiandone periodicamente la password e se possibile attivando l'autenticazione a due fattori. Questo sistema, oltre alla login classica nome utente/password, utilizza per l'autenticazione un secondo passaggio di controllo e conferma, che può essere, ad esempio, l'invio di un codice di verifica su un altro device già autorizzato o un SMS sul numero di telefono associato all'account. Questo codice dovrà poi essere inserito a conferma di un nuovo accesso all'account mail da un nuovo dispositivo (es. computer, smartphone) rendendo più difficile violarlo.



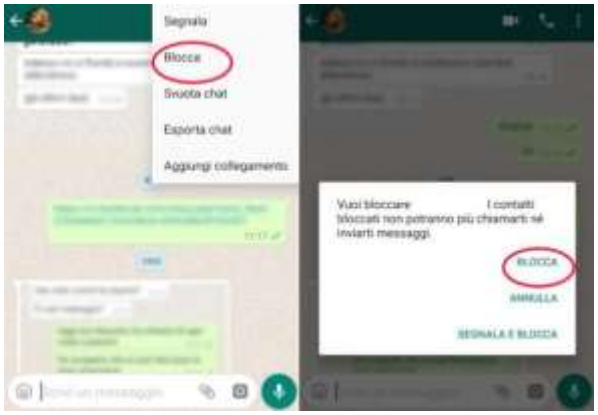
Tutti i maggiori servizi di posta elettronica, gratuiti o a pagamento, includono oltre alla possibilità di filtrare i messaggi in arrivo, anche il filtro antispam. Questo fondamentale servizio, utilizzando database centralizzati e condivisi ed intelligenza artificiale, identifica i messaggi di spam (circa il 90% di quelli circolanti in rete) e quelli di phishing, e li raccoglie nella cartella *spam.* Inoltre, se si apre il messaggio, il filtro disattiva i link ed i contenuti esterni presenti e segnala in modo ben visibile la criticità. Visto che questi sistemi imparano a riconoscere indirizzi e contenuti sospetti anche dal nostro comportamento e segnalazione, non esitiamo a segnalare il messaggio come spam per proteggerci in futuro. Nel tempo molti database di provider di servizi di email sono stati violati e gli indirizzi, con credenziali e dati personali associati (incluse password) sono stati pubblicati o venduti sul dark web, non solo resta fondamentale cambiare periodicamente la password di accesso all'account, ma in caso di account vecchi, non più utilizzati, conviene cancellarli perché spesso, una volta violati e infettati dai malware diventano involontario veicolo di ulteriore propagazione di virus, phishing e spam.

3.2.7. Proteggere i propri dati sui social network

L'utilizzo dei social network sta diventando sempre più comune e spesso le persone hanno attivi contemporaneamente più profili su più social (Facebook, Twitter, WhatsApp, Instagram, Linkedin, TikTok, ecc.). In generale le regole principali per proteggere i propri dati sui social network sono:

- utilizzare una password forte (alfanumerica di una lunghezza adeguata con maiuscole/minuscole, numeri e caratteri speciali) e non condividerla con nessuno.
- Non utilizzare la stessa password per più profili o servizi, nel caso ci siano problemi di memorizzazione delle molte password è possibile usare un software di password management (portachiavi) descritto in precedenza.
- Accettare richieste di amicizia solo da persone conosciute – prima di accettare una richiesta di amicizia o *seguire* qualcuno, verificare con uno o più messaggi l'identità del richiedente, guardare la sua *time-line* e che genere di contenuti condivide; nel dubbio non accettarla.
- Non condividere informazioni personali con chiunque; anche dati sensibili quali grado di istruzione, affiliazione politica, posizione lavorativa o simili, possono sembrare dati non importanti ma in realtà possono essere utilizzati per ricavare altre informazioni o possono portare a inserzioni pubblicitarie non volute.
- Fare attenzione a pubblicare qualcosa che possa danneggiare la propria reputazione o compromettere l'immagine; si dice che una volta che viene pubblicata su internet una foto (un documento o un post), ci rimane per sempre.
- Impostare correttamente la propria privacy mantenendo le proprie informazioni personali accessibili solo *da te stesso*; la maggior parte delle opzioni di default permettono invece la condivisione di informazioni personali con gli altri utenti.
- Disattivare la geo-localizzazione all'interno del social network per evitare inserzioni pubblicitarie e tracciamento continuo della propria posizione.
- Pensare bene prima di condividere una foto personale: è riconosciuto come un potenziale rischio per la sicurezza per chi o cosa è presente nella foto, oltre a dare preziose informazioni ai cybercriminali o agli inserzionisti pubblicitari.
- Quando viene visualizzato un pop-up o è presente una dicitura del tipo *clicca qui per visualizzare più informazioni sul tuo artista preferito* o similari, quasi sicuramente c'è una app di terze parti che viene eseguita; nessun Social network si assumerà le responsabilità nei confronti di queste app e quindi occorre prestare estrema attenzione.
- Non eseguire il login al social network da un computer pubblico, dal telefono di un amico, dalle reti wi-fi sconosciute.
- Fare attenzione ai messaggi che contengono link dubbi, anche se provengono da *amici* conosciuti in quanto potrebbe trattarsi della violazione del loro account per diffondere, a loro insaputa, un malware alla cerchia degli amici e dei contatti.

Importante e fondamentale in caso anche solo di sospetto abuso fraudolento da parte di altri la segnalazione, il blocco e l'eventuale denuncia del fatto.



In molte applicazioni di messaggistica e social networking sono presenti specifiche funzionalità per la segnalazione o il blocco di messaggi ed utenti che rappresentano potenziali minacce. Ad esempio su WhatsApp sono presenti entrambe le opzioni (segnala e blocca) ed anche Facebook prevede queste funzionalità.

Risulta piuttosto evidente che l'utilizzo di uno o più Social network finalizzato alla condivisione delle informazioni personali quali ad esempio luoghi visitati, eventi, hobby, amicizie, ecc. è in antitesi con il concetto di privacy, che caratterizza invece l'abito circoscritto e custodito della vita personale e privata di un individuo. Visto che l'utilizzo dei Social network è molto diffuso e tante persone che amano rendere pubbliche le proprie informazioni personali, risulta particolarmente importante prestare attenzione alle regole indicate nel presente paragrafo, in modo da minimizzare i rischi che qualche malintenzionato possa utilizzare tali informazioni per recare in qualche modo danno ai legittimi proprietari.

Questo è ancora più vero quando le informazioni appartengono a dei bambini che sono particolarmente esposti e vulnerabili ai rischi che si corrono utilizzando in modo inappropriato tecnologie ed internet. I giovani che sono nati nell'ultimo decennio stanno crescendo a stretto contatto con le tecnologie dell'informazione e devono essere educati ed accompagnati dalla famiglia e dalla scuola nella scoperta del mondo digitale, costì come avviene per il mondo reale.

È fondamentale garantire che i bambini, come gli adulti, traggano vantaggio dal coinvolgimento nell'ambiente digitale e mitighino i danni associati, come indica anche, dal marzo del 2021, un nuovo Commento Generale alla *Convenzione internazionale sui Diritti dell'Infanzia* dell'ONU. Per genitori ed educatori sono disponibili tantissimi approfondimenti on line a partire dal sito del Garante dell'infanzia o dal video promozionale sui Diritti dei nativi digitali: https://youtu.be/YWg-d8WPXk0?list=RDCMUC8Aq3hjeJ75wGUV_wWBFceA .