Antimalware, Antivirus. Sono programmi nati per affrontare i malware e i virus informatici. Rilevano i programmi che generano la minaccia bloccando la loro esecuzione prima che questa abbia causato il danno o cercando di mitigarlo nei limiti del possibile.

Antispam. Sistemi in cloud che intercettano la posta pubblicitaria di basso profilo generalmente indesiderata. Possono intervenire anche sulla sicurezza.

Assessment. Valutazione del rischio informatico effettuata sull'infrastruttura sia a livello tecnologico che di processi.

Autenticazione. Il processo mediante il quale i sistemi verificano l'identità di una persona/organizzazione/applicazione che chiede accesso ad una risorsa. I metodi più diffusi di autenticazione sono le credenziali (username e password o PIN, i certificati digitali, sensori biometrici, smart card, token fisici o App di validazione) che possono essere combinati fra loro per aumentare la sicurezza.

Big Data. Si tratta di un insieme di dati, strutturati o meno, che per quantità, complessità o velocità dei flussi di provenienza, richiedono strumenti, metodi e capacità di analisi particolari. L'analisi dei Big Data può generare molto valore ed è per questo motivo che i venditori di tecnolgia tendono sempre ad inserire "sonde" che poi rendono disponibile una grande quantità di informazioni (spesso legate alla sfera personale) che potranno essere analizzate utilizzate o vendute.

Blacklist. Letteralmente «lista nera». Generalmente un elenco di indirizzi e-mail o IP di mittenti o siti web pericolosi per la sicurezza, utilizzati da sistemi antivirus, antispam o di Cloud Security per bloccare il traffico da essi proveniente o diretto.

Botnet. Una rete di oggetti infetti connessi al web in grado di essere controllati ed attivati da remoto per scatenare attacchi sincronizzati contro obbiettivi designati. Possono far parte di una Botnet: PC, Server, ma anche oggetti interconnessi come telecamere o elettrodomestici wi-fi.

Business Continuity. La capacità di una organizzazione di mantenere la propria operatività, in caso di incidente informatico o altro evento in grado di rendere indisponibili dati e sistemi.

Cloud. Si definisce Cloud tutto il meccanismo di erogazione di risorse (archiviazione o elaborazione) fornito da infrastrutture esterne ed acquistato come servizio scalabile e configurabile.

Cloud Security. L'insieme delle tecnologie e procedure per la sicurezza di dati e infrastrutture in cloud. Definisce anche meccanismi di sicurezza e protezione della navigazione basati su intervento esterno in ingresso e uscita, prescindendo quindi dal luogo fisico da cui si genera il traffico.

Cracker. Persona o gruppo di persone che violando i relativi sistemi di sicurezza guadagnano un accesso non autorizzato ad una risorsa o ad un sistema.

Criptovaluta. Una criptovaluta è una valuta virtuale che costituisce una rappresentazione digitale di un valore, utilizzata come mezzo di scambio o detenuta a scopo di investimento. Le criptovalute possono essere trasferite, conservate o negoziate elettronicamente senza la mediazione di banche centrali o altri organismi di controllo. Le più conosciute sono il Bitcoin, Ethereum, Cardano, Tron. Generalmente le transazioni che riguardano il crimine informatico avvengono tramite l'utilizzo di criptovalute per via della difficile tracciabilità dei movimenti.

Crittografia. Meccanismo matematico attraverso il quale dati archiviati o oggetto di una trasmissione vengono codificati e resi intellegibili solo a soggetti autorizzati in possesso di tecnologia e "chiavi" informatiche necessarie per decodificarli. La cifratura può riguardare indifferentemente file o flussi di dati.

Cryptolocker. Denominazione generica usata impropriamente per definire tutti gli attacchi che cifrano i dati delle vittime per spingerle a pagare un riscatto. In realtà è il nome di uno dei più famosi malware di questo genere, apparso nel 2013.

Cybersecurity. Il complesso delle misure di prevenzione e protezione di tutte le risorse informatiche da minacce di qualsiasi natura come ad esempio furti, calamità naturali, guasti, attacchi informatici, errori umani.

Dark Web e Deep Web. Il Dark Web è una porzione di Deep Web, cioè una parte di www non indicizzato dai motori di ricerca. In particolare il Dark Web è accessibile solo mediante browser specifici e particolari accorgimenti tecnologici che rendono virtualmente irrintracciabile chi naviga e chi pubblica. Per questo motivo, il Dark Web è spesso luogo di attività illecite compresa la vendita di informazioni sottratte con il crimine informatico.

Data Breach. La diffusione o alterazione, dolosa o accidentale, di dati personali. In alcuni casi deve essere notificata all'Autorità Garante entro 72 ore.

Data loss. La perdita definitiva di dati critici (o la loro inaccessibilità a tutti gli effetti) a seguito di un incidente, errori o circostanze non previste. La prevenzione di questo tipo di incidente prende il nome di Data Loss Protection.

Dos o DDos. Attacchi informatici del tipo "Denial of Service" in cui un malintenzionato servendosi generalmente di una Botnet, inonda di richieste una specifica risorsa (ad esempio un sito internet), rendendolo praticamente inutilizzabile.

Disaster Recovery. Si tratta di un progetto di Business Continuity che definisce strumenti e procedure per rispondere in tempi certi ad un grave incidente informatico, garantendo quindi la più rapida ripresa delle attività. Può coinvolgere soggetti esterni all'organizzazione e comportare la stipula di contratti e polizze assicurative.

DNS. È il sistema decentralizzato di risoluzione dei nomi a dominio nel mondo Internet. Una sorta di elenco telefonico che trasforma indirizzi facili da ricordare per gli esseri umani (es. www.univa.it) in indirizzi fisici IP (es. 88.149.206.6). Può essere oggetto di attacchi per dirottare la navigazione su siti contraffatti (DNSPoisoning), oppure può essere utilizzato per prevenire il raggiungimento di indirizzi compromesi (DNS Security).

Firewall. Dispositivo o programma software in grado di montorare e filtrare il traffico di rete. Possono essere posti in corrispondenza della connessione ad Internet dell'organizzazione oppure su singoli terminali.

Hacker. Soggetto o gruppo di persone dedite alla scoperta di vulnerabilità dei sistemi. La definizione non è necessariamente negativa se tali scoperte non vengono utilizzate per commettere crimini.

Impersonificazione. Il complesso delle tecniche attraverso le quali un criminale finge di essere qualcun altro (spesso un VIP) per creare situazioni complesse finalizzate a sottrarre denaro, credenziali o altri dati sensibili. I casi più frequenti si verificano via e-mail ma anche tramite i Social Network più diffusi.

IDS (Intrusion Detection System) – IPS (Intrusion Prevention System). A differenza di un Firewall tradizionale che si basa su liste controllo accessi e regole prestabilite, un sistema IDS controlla dinamicamente il contenuto dei pacchetti in transito e genera un allarme se rileva anomalie secondo modelli prestabiliti. I Sistemi IPS sono invece in grado di bloccare il traffico sospetto in modo automatico.

IoT (Internet of Things). L'insieme di tutti quegli oggetti in grado di connettersi ad Internet esprimendo nuove funzionalità. Ad esempio oggetti domotici, automobili, elettrodomestici...

Mail Merge. La cosiddetta "stampa unione", ovvero la realizzazione di documenti personalizzati utilizzando un testo guida e dei campi variabili, riferiti ad una tabella. In questa guida il termine è utilizzato come suggestione per far capire come sia possibile realizzare una campagna di phishing via e-mail tanto più efficace quanto più sono personalizzati e veritieri i dati utilizzati nella tabella, spesso provenienti da data breach.

Malware. Termine generico per indicare qualsiasi tipo di programma con intenti maliziosi in grado di arrecare danni di qualsiasi tipo, sottraendo informazioni o accedendo illecitamente a sistemi compromettendone la funzionalità.

Man in The Middle – Man in The Mail. Tipologia di attacco molto diffusa per descrivere situazioni nelle quali il criminale informatico si introduce segretamente all'interno di un flusso di comunicazione (ad esempio posta elettronica) carpendo informazioni e documenti che poi utilizzerà per attuare truffe. Spesso questa tecnica viene utilizzata per falsificare fatture inserendo iban in realtà nella disponibilità dell'attaccante.

MDR. Managed Detection & Response. Si tratta di sistemi complessi di monitoraggio continuo della rete di una organizzazione che facendo uso di tecniche predittive e competenze umane è in grado di prevenire o bloccare sul nascere un attacco informatico. Tale funzionalità viene venduta come servizio.

MFA. Autenticazione a più fattori. Inizialmente usata nel mondo bancario, garantisce maggiore sicurezza nell'accesso a risorse a rischio, aggiungendo alle tradizionali credenziali ulteriori meccanismi di validazione come ad esempio codici generati da APP o dispositivi hardware dedicati (token).

Paternità (o non ripudiabilità). Principio secondo il quale ogni documento o processo documentale deve essere associato ad un utente che non deve poter ripudiare o negare ciò che ha firmato digitalmente.

Patch. Letteralmente "pezza". Si tratta di un aggiornamento critico di un programma o di un sistema operativo, che appunto mette una "pezza" a dei problemi di sicurezza o funzionalità. Per tale motivo è estremamente importante che qualunque sistema che lo preveda sia aggiornato con la dovuta frequenza.

Penetration Test (Pen Test). L'insieme delle prove di vulnerabilità di un sistema esposto su una rete. Gli esperti valutano la qualità delle protezioni messe in campo a tutti i livelli e verificano che non vi siano possibilità, allo stato delle conoscenze del momento, di superarle e di prendere il controllo di dati o sistemi.

Phishing. Tentativo fraudolento di ottenere informazioni riservate (generalmente credenziali utente o numeri di carta di credito) ingannando la vittima attraverso indirizzi o siti internet abilmente contraffatti.

Ransomware. Tipologia di malware utilizzato da criminali informatici (spesso gang organizzate) per finalizzare un attacco ad una organizzazione. I dati critici vengono esfiltrati e poi cifrati rendendoli inservibili. Gli attaccanti poi ricattano la vittima richiedendo un riscatto proporzionato alle capacità di spesa, minacciando anche la diffusione dei dati sottratti o altre azioni di vendetta come ad esempio degli attacchi Dos.

RID/CIA. Riservatezza, Integrità e Disponibilità (Confidentiality, Integrity, Availability). Tre parole chiave che racchiudono il concetto di sicurezza informatica che ha quindi il compito di garantire la riservatezza dei dati, la loro integrità e la loro disponibilità al bisogno.

Smishing. Il phishing veicolato attraverso SMS.

Social Engineering. L'insieme delle tecniche psicologiche che spingono la vittima di un attacco a ritenere reale il contesto in realtà contraffatto. Ad esempio un mittente di un'e-mail ritenuto autorevole, un sito perfettamente contraffatto, un SMS ricevuto da un contatto apparentemente reale.

Spoofing. Meccanismo di falsificazione di identità a qualunque livello. Quelli più noti riguardano i mittenti della posta elettronica o di SMS.

Threat Intelligence. La raccolta e l'analisi di informazioni al fine di poter individuare e caratterizzare preventivamente possibili minacce informatiche di qualunque genere in contesti specifici.

Tracciabilità. La possibilità di sapere chi e quando ha agito in lettura, modifica, creazione e cancellazione di un archivio o documento.

VPN. È una tecnologia che permette di raggiungere da remoto la rete interna di una organizzazione facendo uso di credenziali, certificati e crittografia per ridurre il rischio di intrusioni.

Whaling. È una tipologia di attacco phishing mirato espressamente alle alte figure dirigenziali. Facendo leva sul "principio di autorità" o sulla capacità di spesa di questi obiettivi, l'attaccante mira ad ottenere grosse cifre in poco tempo.

Zero-Day. Si tratta di una vulnerabilità non ancora resa nota alla comunità dei tecnici. Può essere utilizzata per anni da diversi soggetti (tra cui agenzie di spionaggio o forze dell'ordine) per intercettare informazioni, oppure essere la porta di ingresso di attacchi improvvisi su larga scala prima che sia disponibile una patch per sanarla.