Normative

Normative

I. Normative per gli amministratori di sistema

Tra i loro compiti:

- Identificazione e nomina degli admin
- Valutazione delle caratteristiche personale
- Diverso profilo giuridico
- Tenuta dei log delle operazioni
- Accessi nominali non generici

II. Normative sul diritto d'autore

Due possibili vie d'uscita:

- **Software Open Sourc**e: Sw distribuito con licenza che permette la libera distribuzione in forma di sorgente e che l'utente può modificarli e ridistribuirli.
- **Creative Commons**: Licenze con 4 possibilità
    - By: Il merito deve essere attribuito al creatore
    - Nc: Non è consentito l'uso commerciale
    - Nd: Non sono consentite modifiche o adattamenti
    - Sa: Gli adattamenti devono essere condivisi alle stesse condizioni

III. GDPR

Regolamento UE che deve essere recepito e integrato con la normativa locale. Dice alle aziende **cosa debbono fare e non come**. Misure adeguate che devi valutare quali siano in relazione alla tecnologia corrente e al rischio dei dati.

- Il **Data controller**, il titolare, è responsabile dei trattamenti che avvengono e può designare specifici compiti e funzioni.
- Il **Data processor**, il responsabile, è colui che tratta i dati. Ha la responsabilità giuridica dei suoi trattamenti.
- **Dati personali**, Tutti quelli che conducono all'identità di una persona. nome, #telefono, indirizzo, ip, cookies, codici imei.
- **Dati speciali**, sensibili, Informazioni relative a razza, idee politiche, religiose, dati genetici, biometrici.
- L'utente deve avere i **diritti** di Copia, Correzione, Cancellazione, Trasferimento e Sospensione dei dati.
- **Base giuridica**, motivo che permette il trattamento dei dati.
- I dati raccolti devono essere usati per il fine esatto e limitati al minimo necessario. Il tempo di conservazione deve essere specificato nel consenso.
- **72 ore**, tempo entro cui le violazioni devono essere segnalate all'autorità competente e eventualmente anche agli interessati.

Fattore umano

Fattore umano

Le regole imposte con la paura non funzioneranno, meglio la riduzione del danno. Molti temi tecnologici hanno la controparte umana. Attaccare DataCenter è sempre più complesso, è più facile provare a passare dal client → **Anello debole della catena**.

Alcuni dei problemi di base non tecnologici:

- Fallibilità esseri umani
- Tendenza naturale alla fiducia
- Interfacce complesse
- **Shadow IT**: App consumer migliori e più funzionali di quelle aziendali, vanno incontro alle esigenze dell'utente, ma portano a problemi di sicurezza.
- **Byod**:

Bring your own device: Declinato in vari modi (technology, pc, phone), Due scuole di pensiero: **Cope** (Company owned, personally enabled), **Poce** (Personally owned, company enabled). È necessario definire i limiti e modi di utilizzo, responsabilità aziendali e personali, servizi, app che devono essere accessibili, misure di sicurezza, monitoraggio.

Social Engineering

Sfruttare la partecipazione dell'utente per un attacco. Attaccare i **punti deboli** dell'utente, pressione psicologica. Diversi canali di attacco (mail, phone, usb). Richiede una fase di studio, analisi. Dimostrare di conoscere l'azienda, porta ad abbassare la guardia. I punti deboli possono essere:

- Stabilità dei comportamenti
- Validazione sociale
- Liking, dare fiducia a chi simpatico
- Sudditanza verso autorità vera o presunta
- Sovrastimare il valore di cose scarse
- Reciprocità, Paura, Ignoranza

SPAM

Pubblicizzare prodotti a scopo commerciale o phishing per portare il destinatario a visitare siti o pagine compromesse per catturare dati. Danni economici, ma anche in tempo.
Strumenti come **Antispam**

- Filtri sui contenuti, probabilistici e sempre un passo indietro
- Black- White listing mittenti, aggiornamento liste, e dos per mittenti inconsapevoli
- Greylisting, temporary error
- Sender Policy Framework, controllo incrociato dell'ip
- Dkim, il proprietario certifica la responsabilità della mail
- Dmarc, Dkim, Spf, e regole.

Mail Marketing: Le mail non richieste. Una mail non finisce come spam se il server di invio ha una buona reputazione (non infastidire i domini target) o il messaggio non deve essere fastidioso per il target.

Phishing: Lancio di molte esche, sperando che qualcuno abbocchi. Whaling quando è mirato a cio/ceo e molto sofisticato. Spear phishing quando mirato a gruppi potenziali canali di intrusione. Es: scaricare file, aprire link, app che simulano un login, browser in browser.

Difesa: Consapevolezza dell'utente, url accorciate, mail invece dei nomi, diffidare da mail strane, richieste varie.

Password: Cambio solo se compromesse. Password manager e ricordare solo la master p. Più vincoli si impongono vincoli, meno tempo per attacchi di forza bruta. Alcune delle nuove regole da utilizzare sono: Length 8-64, Tutti i caratteri, No a domande di recupero.
Non vi devono essere segreti personali, non verità, non deve avere senso e non prevedibile. L'autenticazione a 2 fattori prevede qls che so (password), e qls che ho (token). I token fisici sono scomodi e poi vi è il problema dell'allineamento dei clock. Due possibili attacchi:

- Dos: con errori di chiave
- Social Eng: per sostituire la chiave.

Passkey: Serve che il sito, browser, password manager e OS che le supportino. A2Factor senza password.

- L'utente deve confermare le informazioni dell'account e presentare le proprie credenziali. Una chiave privata viene generata in base alla chiave pubblica fornita dal sito web. La chiave privata è memorizzata sul dispositivo.
- Quando l'utente tenta di accedere a un sito Web, utilizza la chiave privata generata. Seleziona le info dell'account e presenta le credenziali per sbloccare la chiave privata. Di conseguenza, non vi è alcun rischio di fuga di password poiché nei db dei siti non vengono archiviate password.

Privacy

Privacy

- **Sicurezza**: cose fatte contro la mia volontà
- **Privacy**: azioni che eludono la mia volontà
- **Reputazione online**: cose che succedono secondo la mia volontà involontaria. (Se è volontà volontaria si chiama “branding”)

È un concetto che muta nel tempo, nello spazio e può essere diverso a seconda della cultura. Il primo approccio giuridico “The right to privacy” del 1890, uno dei saggi del diritto US. Due visioni:

- **FIP**, fair information practices: Presuppone la legittima necessità statale di raccolta dati per fini amministrativi (UK)
- Privacy come **diritto umano fondamentale** (UE)

Come **finiscono online** le info:

- I telefoni eseguono dei **probe request**, cercano le reti già note per collegarsi, si ricostruisce la storia del telefono, si risale all’abitazione del proprietario
- **Tracciare utenti indoor con wifi** (802.11 az) con precisione di metri (uso anonimo in aeroporto e punti di interscambio)
- Totem in centri comm. o stazioni con telecamere. Possono essere collocati sw e eseguire trattamenti dati per l’area marketing, come gradimento della pubblicità, fasce orarie.
- **Fotografie**: registrano informazioni come data, ora, tipo fotocamera, gps
- **Codici a barre bidimensionali**, contengono dati
- **Spegnere il gps non aiuta**. Il telefono può trovarci in pochi minuti
- Strumenti basso costo, bassa sicurezza
- **Dispositivi attaccabili da remoto**, con bluetooth, telecamere, microfono.
- Osint, Open Source Intelligence: Raccolta di informazioni in rete per attacchi social eng.
- **Google dorks**: Google indicizza tutto, se è su google, anche i cattivi possono trovarlo. Tramite query avanzate si possono scoprire informazioni. Come: allintext:username filetype:log
- **Scansionare siti** per raccogliere informazioni

Pymk di Meta: Alg misterioso con: user nello stesso posto, che si muovono insieme, imperfezioni simili nelle foto, persona in rubrica. Dati acquisiti da esterni e quelli suoi, 30k categorie disponibili per fare profilazione.

Telefoni che ascoltano: sarebbero tanti dati da gestire, analisi del testo locale, cpu, linguaggio ambiguo. Non ascolta, ma invia dati anche quando non viene usato.

Anonimato non esiste: bastano dei punti di incrocio e salta tutto.

Se è gratis: il prodotto l’utente. Il valore sono le informazioni. I term of service sono lunghi e complessi da leggere. I guadagni sono grazie alla pubblicità.

Data broker: Aziende che guadagnano vendendo i dati di utenti.

Google permette non di rimuovere dati dal sito, ma non comparire nei risultati di ricerca.

Cookie

Meccanismi per mantenere la sessione. Esistono vari tipi:

- Sessione: Relativi alla sessione, si eliminano alla chiusura
- Persistenti: Rimangono fino alla scadenza
- Secure: Per gestire i login, solo via https
- Preference: Per memorizzare le preferenze
- Statistics: Stats di navigazione
- Terze parti: Per tracciare la navigazione dell’utente. Possono essere disabilitati.

Proposta alternativa: Topics. Fornisce indicazione generiche agli inserzionisti sulla profilazione dell'utente basandosi sulla sua navigazione per categorie.
La normativa include: Possibilità di rifiuto, no a cookie wall, no silenzio assenso.

Si riesce a identificare un browser da: User agent, DIM schermo, Font- Estensioni- Plugin installati, Timezone, lingua

Per mitigare il rischio: Gestire le impostazioni del browser, proteggere la webcam, esercitare il diritto di accesso ai dati, georeferenziazione foto-phone-auto, Https, Vpn, OpenDns

Cattivi

Chi sono i cattivi

Solo conoscendo i nemici online si evita di diventare vittime.

I cattivi **non sono sempre perfetti**. Quelli isolati sono più difficili da scoprire e possono esporsi quando muovono soldi.
Tra i non professionisti, sempre +giovani e +frequenti. Mancanza della percezione del digitale come mondo basato su regole. A volte solo per divertimento- sfida.

- Il **bersaglio**: inizia con l'idea di non essere tale, ma magari è solo la sponda per colpire altri. Gli ATT possono puntare a un colpo da 1M o 100k da 10.
- Il **nemico**: Non sempre è fuori, non è sempre cattivo, e può non sapere di essere il nemico. I meccanismi dei cattivi non professionali sono più complessi di quelli esterni.

Prima di commettere un illecito: valutano i pro-contro, le conseguenze.
La **dinamica criminale** prevede **5** fasi:

- **Motivazione** a compiere l'azione
- **Fantasia criminale**
- **Anticipazione mentale degli effetti** dell'azione. Punto chiave su cui agire per difendersi
- **Progettazione** e **Esecuzione** del crimine.

Nel computer crime non vi è il contatto tra vittima e ATT. Tra reato e oggetto del reato.
Cambia l'anticipazione del reato. Riduco l'analisi dei pro-contro.
L'oggetto digitale:

- **Non rivale**: uso contemporaneo di più persone
- **Non esclusivo**: debbo fare qualcosa per proteggerlo altrimenti è sprotetto di default
- **Costo marginale nullo**: fare #copie senza costo.

Come un bene pubblico, ma la legge si applica.

Si **allarga la base dei possibili autori** di reato rendendo adatti al crimine anche soggetti normalmente estranei al mondo della criminalità.
Crea un fenomeno di **illegalità distribuita** in larghe aree sociali.
Diffonde un falso **senso di impunità** su determinati crimini

Sicurezza software

Sicurezza software

Hardening di sistema: Tecnica di configurazione dei sistemi per **aumentarne la sicurezza** intrinseca. Ciascun server richiede le proprie tecniche.

Tecnica del **Less is better**: Lasciare solo i servizi indispensabili. Tra le tecniche vi è:

- Disattivare programmi non usati
- Controllo delle configurazioni del sw, e dei permessi
- Configurare i parametri di sistema.

Obiettivo comune è ridurre la superficie di attacco.

Il patch management prevede varie fasi, ma effettuarla o no dipende dal fatto: il rischio di applicare al sistema la patch > rischio della vulnerabilità che la patch corregge?

App web

Il software rimane vulnerabile perché i vantaggi dei prodotti non sicuri > degli svantaggi.

Il problema di base è che i servizi web sono esposti al mondo, sono personalizzati e complessi. Con una struttura a tre livelli (web, app, db). Possono poi essere ridotti con l'uso di librerie.

Le **vulnerabilità** possono nascere da:

- Sviluppo, user request, CDN
- Comunicazione via api, Interazione con backend- database server.

Sicurezza:

- **Sicuri come l'anello più debole**
- Ciascun utente, componente deve avere i **privilegi strettamente necessari**
    - Es: accesso al db con solo alcune necessità. I comandi come drop table dovrebbero essere inibiti.
- Separazione: **componenti diversi che accedono a dati diversi** (complessità)
- **Chiamate di sistem**a portano il controllo da app a SO
- **Validare input o output**
- **Gestire gli errori in sicurezza**. Non fornire troppe informazioni (commenti)
- **KISS**, meccanismi di sicurezza devono essere semplici
- **Riusare** componenti già testati.
- **Esporre solo il necessario**
- **Mai fidarsi dell'utente**

Data validation: Accettare solo i dati validi. Controllare il tipo, la sintassi, la lunghezza. Lato client per prime scremature e ri-controlli sul lato server.

Metacaratteri: Caratteri speciali che possono essere pericolosi. <>, ../, !|&;,

Directory Traversal: Percorrere il file system del web server con caratteri speciali e privilegi errati.

SQL injection: Iniettare codice malevolo nei campi di un form, query. Problemi nel caso in cui si usa l'input direttamente nelle query.

HTML injection oppure command inj. quando il codice web richiama comandi di sistema.

XSS: App che emette in output codice html non verificato e contenente dati immessi in input dal client. L'ATT può inserire codice attivo nei documenti inviati al client usando il server come sponda. Varie tecniche: indurre l'utente a visitare pagine di quel server con codice html malevolo senza che se ne accorga.

Security by design: Integrare la sicurezza in tutto il ciclo di vita del progetto. Non deve essere una cosa separata. Non deve esistere un documento della sicurezza separato. Tenerne conto solo alla fine ha costi elevati. Fin dall'inizio:

- Analizzare tutte le esigenze degli stakeholder, Valutare l'impatto del contesto, Le minacce correnti e passate,
- Rischi e i corrispondenti modelli, Costruire fin dall'inizio un modello di gestione dell'incidente.

Anche dopo la fine dello sviluppo: Checklist, pen testing a terze parti, strumenti come secure code review.
I problemi vanno risolti. **Security by Obscurity** non funziona. Non sperare che non vengano scoperti.
Bug:

- **Design**: diffusi, complessi e costosi.
- **Implementazione**: locali, semplici, ricorrenti. Per prevenire si può usare il meccanismo poka yoke, progettare pezzi per cui sia impossibile sbagliare.

Per mitigare il rischio:

- Identificare i security requirement, Liste di controllo, Linee guida
- Generare "abuse case", Security pattern, Simulare modelli di attacco
- Framework di sviluppo sicuro, KISS

Librerie: Sono un problema perchè manca il **Sw bill of material**. La struttura a cascata di tutte le dipendenze. Es: stack tcp/ip che vengono riusati ma si scopre bucato anni dopo.

Owasp: organizzazione per promuovere lo sviluppo di sw sicuro con: documentazione, sw, gruppi di lavoro, formazione.
Attacchi alla catena di distribuzione del software.

- Sui grandi sw intervento di attori statali
- Attacco ai certificati che garantiscono il SW
- Inserirsi all'interno del flusso degli aggiornamenti
- Sfruttare il codice aperto per inserire backdoor ecc.
- Modificare app sullo store, meglio ancora se framework di sviluppo.

Sicurezza fisica

Per la disponibilità del dato **è necessario anche proteggere il device fisico** che lo contiene. Armadi e sale con **controlli a più livelli**, **sistemi di controllo diversi**. Accesso solo per le **persone autorizzate**. Protezione **contro fuoco, acqua, calore ∆corrente elettrica**, ventilazione.
Proteggere l'hw prima che arrivi al destinatario. Per stati- governi- grosse aziende vi è il problema dei fornitori. Proteggere chi mette mano al dispositivo.
Tramite usb:

- Dispositivi che simulano una tastiera e scrivono le credenziali dell'utente
- Usb kill con condensatori, nata come proof of concept
- Cavi che si collegano via wifi a un host remoto e prende possesso mentre si carica.

IoT

IoT

Internet delle cose, **tutto ciò che è connesso è attaccabile**. Sistemi a basso costo. Quindi manca la potenza e la sicurezza.
Stuxnet attack: Distribuito tramite usb infette per una compromissione potenziale di impianti nucleari. Richiede un alto livello di competenza.

Mondo IT: Riservatezza → Integrità → Disponibilità. Nel mondo **OT è viceversa**.

IT: Tanti protocolli, Hw-Sw standard, aggiornamenti frequenti, ammissibili degli stop
OT: Protocolli proprietari, Hw personalizzato, Lifecycle lunghi, Lunga durata dei componenti, Sostituzione invece di upgrade, No stop.

CERG: Definisce i target essenziali (come acqua, energia, infrastrutture digitali per banche, salute, trasporti) e quelli importanti (gestione rifiuti, distribuzione elementi, prodotti informatici, disp. medici).
Nell'IoT si usano **parti sw standard** (tcp/ip). Vulnerabilità, e non facilmente patchabili.
Problema delle password. La maggior parte sono quelle comuni.
Vi sono alcuni stati che hanno fatto una legge per vietare i dispositivi che non rispettano i livelli minimi.
ISA 62443: specifica le funzionalità di sicurezza per i componenti del sistema. Fornisce un quadro per affrontare le vulnerabilità della sicurezza nei sistemi di automazione.
Problema degli Aggiornamenti e dell'End of Support:
Per quanto tempo devo tenerlo. L'EoS va bene nel mondo IT, ma nel mondo IoT forse no. Una casa automobilistica che produce 2-3 modelli all'anno si potrebbe trovare a dover mantenere decine di versioni diverse di software che, essendo IOT, va poi testato con i veri componenti HW.
Auto: Sono processori collegati da uno o più CAN bus. Architettura semplice, basso costo, traffico non crittografato. Accessibile smontando i fari. Possono essere usate le porte per accedere al bus. I sistemi keyless sono attaccabili con estensori del segnale radio.
ISO 21434: Standard per la cybersecurity delle auto. Vuole che tutti gli attori del settore automotive (costruttori, fornitori) abbiano la consapevolezza dell'importanza della sicurezza nel processo di sviluppo, realizzando la security by design.
Poi il problema dei dati raccolti dai sensori. I dati possono essere venduti a information broker.

Spoofing HTTP - Attacchi Omografi IDN

Spoofing HTTP - Idn Homograph attack

HTTP Spoofing è quella tecnica malevola che sfrutta l'http. Gli attaccanti creano dei siti web che sembrano uguali a quelli reali, ad esempio mostrando il lucchetto e il prefisso "https://" facendo così credere agli utenti che si tratti di un sito sicuro e affidabile.

Per fare questo vengono sfruttati gli IDN. I nomi di dominio internazionalizzati, che vennero proposti nel '87 e implementati nel '90, hanno permesso l'uso di tutti i caratteri Unicode nei nomi di dominio. Questo ha migliorato l'accessibilità per gli utenti di diversi alfabeti, ma ha introdotto questa vulnerabilità inaspettata.
Omografo IDN è il termine per descrivere due domini internazionali che sembrano uguali, ma composti da caratteri diversi. Questo viene reso possibile dal fatto che alcune lettere di alfabeti non latini (greco o cirillico) assomigliano molto alla lettere ASCII.
L'attaccante può quindi registrare un dominio che include IDN e usare questo dominio per fare attacchi di phishing, spingendo le persone ad aprire il sito falso creato.
Anche prima dell'introduzione di IDN, lo spoofing HTTP era possibile, ma individuabile più facilmente. Ad esempio un attaccante avrebbe provato a registrare "0nedrive.com" anziché "onedrive.com", ma osservando la barra degli indirizzi ci si poteva accorgere subito dell'errore e porre attenzione.

Gli attacchi che possono essere effettuati sono quindi Phishing o Man in the Middle.

- Phishing, sfruttando le vulnerabilità psicologiche degli utenti, cercando di far interagire le persone con siti che sembrano affidabili
- Man in the middle, intercettando comunicazioni tra il dispositivo di un utente e il server di un sito, posizionandosi in modo invisibile tra le due parti.

Lo spoofing ha conseguenze anche dannose. Ad esempio:

- Furto di dati, possono appropriarsi delle credenziali di accesso e dati personali, portando a violazione di privacy.
- Danni alla reputazione, i clienti di aziende che subiscono attacchi di questo tipo possono perdere stima verso di loro e verso la loro capacità di proteggere i dati.
- Malware, possibilità di distribuire malware e utenti inesperti possono scaricarli sui loro dispositivi.
- Conseguenze legali, aziende che sono incapaci di proteggere i dati degli utenti possono portare a violazioni di normative come GDPR o HIPAA (Health Insurance Portability and Accountability Act, legge federale degli USA che definisce i requisiti per il trattamento dei dati sanitari protetti dei privati).

Il Punycode è un codice per rappresentare caratteri Unicode come caratteri ASCII nel dominio. Tutti gli IDN sono archiviati ed elaborati come Punycode e visualizzati solo nel formato Unicode per gli utenti. Quando un utente visita un url IDN, il browser lo converte in Punycode e dopo invierà informazioni ulteriori.

I modi per prevenire gli attacchi sono l'uso di un browser moderno, controllare sempre la barra degli indirizzi, in quanto mostrerà il nome falsificato in Punycode che non assomiglierà al nome originale legittimo, oppure l'uso di password manager abilitati per il web in modo che completino gli indirizzi solamente se il dominio corrisponde a quello archiviato.

I. https://www.invicti.com/learn/mitm-https-spoofing-idn-homograph-attack/
II. https://www.punto-informatico.it/che-cosa-si-intende-spoofing-https/

Tutto

All in One

1) Attacco informatico: azione che compromette la confidenzialità (che il sistema fornisca i dati solo agli autorizzati), integrità (che il sistema fornisca i dati in formato inalterato) e la disponibilità (che il sistema fornisca i dati quando previsto a chi può- deve fruirne) delle informazioni.

2) Gordon Loen: Un'azienda per mettere in sicurezza i propri dati quando dovrebbe spendere viene detto dal modello di Gordon Loeb. Ovvero il 37% del valore dei danni in caso di perdita dati. Questo è il valore ottimale che dovrebbe spendere e si ottiene analizzando l'andamento del rischio e della sicurezza in funzione dell'importo speso. Infatti all'aumentare dell'importo, la sicurezza aumenta, mentre il rischio cala, ma rimane sempre un rischio residuo. Questo può essere coperto con le assicurazioni, quindi pagando un certo premio a seconda del valore del RR. Per i modelli di sicurezza si fa riferimento allo Swiss Cheese Model, in cui ogni strato riduce il rischio ma non lo azzera. Quindi se vengono usati più strati, quello che non intercetta uno, si spera lo intercetti il successivo. Tra ATT e DC vi è un'asimmetria. L'ATT è nel dominio del guadagno, investe per guadagnare. Il DC è nel dominio delle perdite, lui investe per non perdere. Il DC non è detto che faccia la scelta più razionale, ma quella che lo porta a soffrire di meno. I rischi li deve valutare anche l'ATT, in quanto deve valutare il valore del target, deve usare del tempo per studiarlo, per attaccarlo.

3) Complessità: La sicurezza è nemica della complessità. Infatti per aumentare la sicurezza è meglio ridurre la complessità. Questo può essere fatto aumentando la standardizzazione, quindi cercare di usare più prodotti simili tra loro, sfruttando la tecnologia. Oppure migliorando la gestione dei processi, con nuovi modelli organizzativi. La soluzione ideale sarebbe quella di strumenti sicuri, semplici ed economici, ma se ne possono scegliere solo due.

4) ISO27001: Specifica tutti i requisiti per mantenere e migliorare un sistema di gestione della sicurezza. È uno standard generico che riguarda tutte le organizzazioni, sviluppato in checklist. Annuale. NIST Framework: Guida volontaria per gestire la sicurezza e ridurre al minimo i rischi. DORA: Guida UE per gli istituti finanziari.

5) Le analisi preventive sono: Scansione (in cui si raccolgono i dati, e può essere anche automatica), Assessment (si consolidano i dati e valutano i FP), Penetration test (si fa l'exploit delle vulnerabilità, si prova a bucare il sistema).

6) Backup: Consiste nel salvataggio dei dati seguendo precise policy. (Archiviazione che è il salvataggio di dati statici). Possono essere: FULL (Si salva sempre tutto. Il contro è lo spazio necessario), Incrementale (Salvo le differenze rispetto al precedente, che sia full o incrementale stesso. Ad esempio: FULL alla domenica, e ogni ogni giorno salvo la differenza prima rispetto al FULL, e i giorni successivi rispetto al precedente. Funzionamento in catena, se si rompe uno, si hanno problemi con i successivi), Differenziale (Salvo le differenze sempre rispetto l'ultimo FULL. Funzionano in coppia, se si rompe il FULL si avranno problemi). Prevedono poi la regola del 3 (copie del dato), 2 (media diversi), 1 (copia in un luogo separato), 1 (copia su un altro cloud, fuori linea), 0 (errori durante il processo).
Si possono usare due intervalli temporali: RPO (recovery point objective, tempo tra l'ultimo istante disponibile e il disastro), RTO (recovery time objective, tempo tra il disastro e quando il sistema alternativo torna disponibile). L'obiettivo è ridurli in modo da ripristinare in poco tempo il Business Continuity.

7) Il Disaster Recovery Site: È un centro servizi remoto che contiene tutti i servizi, applicazioni, dati, necessari all'azienda nel caso di attacchi o indisponibilità per ripartire. Vi è poi il Piano di DR, che contiene la descrizione del sito. Personale da contattare, procedure.

Deve quindi essere mantenuto disponibile, aggiornato, accessibile, ed è importante anche fare simulazioni.
8) Normativa per gli amministratori di sistema: A loro spettano vari compiti. Tra questi identificarli e nominarli; avere un diverso profilo giuridico; valutare le caratteristiche personali; tenuta dei log delle operazioni; gestire gli accessi nominali e non generici.
9) Normativa sul diritto d'autore: Due possibili vie d'uscita. Open Source (software distribuiti sotto forma di sorgenti e gli utenti possono studiarli, modificarli e ri-pubblicare la versione modificata), Creative Commons (Licenza con 4 categorie: BY [Attribuzione, conferire il merito all'autore], NC [Vieta l'uso commerciale], ND [Non prevede modifiche o adattamenti], SA [Condividi allo stesso modo, gli adattamenti]).
10) GDPR: Normativa UE che deve essere integrata con le normative locali. Passa dalle misure minime a quelle adeguate, e dice alle aziende cosa devono fare, non il come. Introduce due figure il Data controller (il titolare, colui che ha l'autorità massima), Data processor (colui che tratta effettivamente i dati). Si parla di dati dell'utente. Questi possono essere Personali (quelli che riconducono all'identità della persona, nome, telefono, ip, cookie, imei), Speciali (sensibili, razza, op. politiche, religiose, dati genetici, dati biometrici). Ogni utente deve avere il diritto di Copia, Trasferirli, Cancellarli, Modificarli, Sospenderli. Le aziende poi possono trattare solamente i dati per cui vi è una base giuridica. Scaduta la motivazione non deve essere più effettuato il trattamento. Le violazioni devono poi essere comunicate entro 72 ore, e se interessano gli utenti, bisogna informare anche loro.
11) Ransomware: Attacco in cui si prendono in ostaggio i dati dell'utente, vengono cifrati e si richiede un riscatto per consegnare la chiave. I pagamenti sono in genere in criptovalute, ritardare il pagamento spesso non porta ad avere la chiave. I canali di attacco possono essere applicativi infetti, o link malevoli. Ci si salva con buoni backup fuori linea. Il ripristino avviene tra week- month. Si possono puntare tanti piccoli incassi (A pioggia) o al colpo mirato.
12) Denial of service: Attacco in cui si impedisce il funzionamento di un servizio con attacchi da più punti della rete. Le motivazioni possono essere per Hacktivism, Riscatti, Bloccare un servizio per attivarne altri. Può essere effettuato in vari livelli (Syn flooding, Trasporto, oppure si fa il ping di una rete intera chiedendo risposte grosse).
13) Man in the Middle: Attacco con l'inserimento all'interno della comunicazione per ascoltare il traffico, intercettarlo. (Mail ITM).
14) Privilege escalation: Quando si tenta di accedere a un sistema con privilegi maggiori di quelli previsti per l'utenza. Dovuto a errori di programmazione.
15) Backdoor: Porte di servizio rimaste aperte per errore o volutamente.
16) Keylogging: Intercettare i caratteri che vengono digitati sulla tastiera.
17) Buffer overflow: Quando si accede ad aree di memoria che non dovrei vedere. Va a sovrascrivere l'area di memoria del puntatore di ritorno per mandare in esecuzione una shell di root.
18) Command e Control: Rete di server che controllano macchine infette, zombie. Si spostano velocemente e sono difficili da intercettare. Usano protocolli standard e connessioni crittografate, ma con organizzazioni complesse dietro.
19) Advanced persistent Threat: Attacchi che non puntano a un obiettivo immediato, ma ad installarsi nella macchina target e rimanere nascosti esfiltrando dati per lungo tempo oppure fino al momento di esplodere. E possono sfruttare command e control.
20) Protezione rete ethernet: Può essere fatta con Mac locking (blocco delle porte con access control list sul mac address), Acl locking (blocco delle porte con regole più sofisticate)

21) 802.1X port authenticator: È il meccanismo che impedisce l'instaurarsi del collegamento fisico finchè non è stata completata una fase di autenticazione. Richiede che i dispositivi lo supportino (possono essere problemi con vecchi dispositivi, come v. stampanti). Vi è il supplicant che viene inserito in una vlan in cui vi è solo l'authenticator. Viene effettuata l'autenticazione con EAP (EAPOL: eap over lan). EAP è il framework che definisce i metodi di autenticazione, non un protocollo di rete, ma solo i messaggi che vengono scambiati. Per il protocollo di rete deve essere incapsulato. EAP: MDS (user/password), TLS (certificati digitali), TTLS (user/password e certificato). L'authenticator chiede al server centrale tramite il Radius la verifica. E se è corretto allora il supplicant è connesso. Radius è un authentication server con le funzioni Authorization, Authentication, Accounting, Auditing.
22) Protezione rete wireless: WEP sconsigliato perché insicuro. WPA (Wifi protected access) in versione Personal (per le reti domestiche, dove ogni utente si autentica con la stessa chiave generata da una password), Enterprise (versione aziendale, dove è richiesto il radius). WPA3, in cui vi è un aumento della length della chiave (128, 192 a seconda della versione Prs, Etp), e con una gestione dinamica delle password per rendere inutili gli attacchi offline.
23) Rogue: Il Rogue Access Point è punto di accesso wireless che può essere installato in una rete, il tutto per fini legittimi o dannosi. Può essere usato per motivi interni o di test. Oppure per attirare i dispositivi degli utenti e fare attacchi Man ITM, o per Phishing re-indirizzando gli utenti a siti falsi o per accedere a reti aziendali bypassando i controlli di sicurezza. Possono essere difficili da individuare. Rogue Cell Phone Station, lo stesso ma per le reti smartphone. Le reti cellulari più vecchie (GSM e in alcuni casi 3G) non implementano crittografia forte, rendendo più semplice l'intercettazione. I fini principali sono: Monitoraggio di chiamate, SMS, dati e posizione.
24) IP Spoofing: È quella tecnica che permette di modificare l'ip sorgente, facendo credere che quello provenga da un'altra parte. Non può essere fatto con uno stack ip standard, ma può essere la base per attacchi.
25) Syn flooding: Protocollo TCP a tre strati: Syn (inizio), Syn-Ack (conferma), Ack (completare). Può portare a esaurire le risorse di un server (DOS). Ci si difende inserendo dei timeout, non troppo corti né lunghi. Funzionamento normale: Client invia un Syn, Server risponde con il Syn-Ack, e il Client invia l'Ack. Un cattivo potrebbe inviare tanti Syn e non rispondere ai Syn-Ack del server. Il Server rimane in attesa dell'Ack, ma questo non arriverà. I Server hanno uno spazio limitato per le connessioni, questo si riempie e non potrà più accettare nuove connessioni. Ridurre il timeout, significa che il server chiuda più rapidamente le connessioni incompiute. Timeout lunghi: Le connessioni aperte rimangono per molto tempo, e i server sono più vulnerabili e gli ATT possono usare un #ridotto di pck. Timeout brevi: potrebbero essere chiuse connessioni legittime che impiegano più tempo.
26) Arp spoofing: Attacco che usa le vulnerabilità del protocollo Arp. L'attaccante invia risposte ARP false sulla rete, associando il proprio indirizzo MAC a un determinato indirizzo IP (ad esempio, quello del gateway o di un altro dispositivo). La vittima invia il traffico all'attaccante invece che al gateway. L'attaccante può: Intercettare e modificare i dati (MITM) o bloccare il traffico (DOS).
27) DNS: È lo strumento che effettua le risoluzioni nome-indirizzo ip. Gli attacchi possono essere: Shadow server (l'attaccante imposta un proprio server DNS maligno in modo che risolva le query in maniera errata, restituendo risposte false o manipolate, portando gli utenti su siti malevoli), Cache poisoning- DNS Spoofing (l'attaccante inserisce nella cache di un server DNS dati falsi per risolvere in modo errato le query successive. Un ATT può sostituire l'indirizzo IP corretto con uno falso, facendolo credere valido), Rispondere a query non

effettuate- DNS reflection (l'attaccante invia query DNS a un server, ma con l'indirizzo IP della vittima come mittente. In questo modo, il server DNS invia la risposta della query, che può essere molto più grande della richiesta, verso la vittima).
28) Domain Hijacking: Attacco che mira a prendere il controllo di un dominio. Si attacca l'utenza di registrazione del DNS. L'ATT può modificare le informazioni di dominio come ip, registrar e altre conf. Questa modifica si propaga in rete, e quando un utente visiterà quel dominio, sarà rediretto alla nuova risorsa. Conviene proteggere l'admin del DNS, con ad esempio un 2 Factor.
29) Dangling Domain: Anche questo mira a prendere il controllo di un dominio. L'ATT può andare a registrare un dominio che un utente aveva registrato e lasciato scadere, dimenticandosene. L'ATT può quindi fare attacchi di phishing, MITM sfruttando questo dominio.
30) Firewall: Sono strumenti hardware e software per isolare parti di una rete. Possono essere: Stateless (Senza memoria, analizzano pck per pck senza discriminare la direzione del colloquio. Le operazioni possibili sono Accept, Deny, Drop), Stateful (Analizzano i pck nel contesto della comunicazione, offrono una protezione maggiore, ma con più potenza di calcolo).
31) Application Level Gateway: Usati nelle reti in cui non vi è routing tra la rete interna da proteggere e quella esterna. Un dispositivo nella rete interna non può aprire una connessione verso l'esterno, ma l'informazione deve passare per un proxy. Il Proxy (HTTP-ALG) disaccoppia l'accesso al web dal browser. Cache proxy: Il browser (in) quando effettua una richiesta per una determinata pagina, questa arriva al proxy che tramite una cache gestisce una copia degli oggetti web richiamabili con una scadenza. Il proxy controlla se nella cache esiste una copia valida e la restituisce, se invece non vi è, allora andrà sul web server a recuperare una nuova copia che la salverà in cache. Reverse Proxy: Ha il compito di sollevare il web server da alcune delle sue funzionalità, come il servire contenuti statici. Content Filtering: Firewall che filtra la navigazione. Con filtraggio degli url, back- white list, filtri dinamici. Zero trust: Si concentra sull'utente e da quale dispositivo si collega. Sposta il focus dal confine, che sta diventando sempre più sfumato e difficile da delineare. In una visione semplificata, l'utente si qualifica con un'autenticazione a 2 Factor, il dispositivo con il certificato, se la coppia ha un sufficiente livello di trust, allora si crea una comunicazione tra utente e app, tutto il resto è deny.
32
33) Shadow IT: È la tecnologia nascosta, quelle app consumer che possono sembrare più performanti agli occhi dell'utente rispetto a quelle aziendali, perché vanno in contro alle loro esigenze. App che possono risultare più efficienti e facili da usare. In quanto, per l'utente, una maggiore sicurezza, potrebbe peggiorare le prestazioni, e potrebbero vedere dei vantaggi in queste tecnologie. Ma se il prodotto è gratis, o comunque a basso costo, la sicurezza sarà bassa o nulla. Usando poi app nascoste, il team IT aziendale perde il controllo sulla gestione e monitoraggio dei dati e anche la perdita di visibilità sulle info aziendali.
34) BYOD: Bring your own device. La lettera D può essere declinata in vari modi: Technologies, PC, Phone. Consiste nell'usare un dispositivo in un doppio contesto. POCE (dispositivi personali, abilitati all'uso aziendale), COPE (dispositivi aziendali, abilitati all'uso personale). Sicuramente vi è da gestire la sicurezza, i limiti di utilizzo e le responsabilità, e quali siano le app e i servizi a cui l'utente può accedere.
35) Social Engineering: Attacco che sfrutta la partecipazione involontaria dell'utente. Sfrutta i suoi punti deboli con meccanismi di pressione psicologica. Attività che richiede una fase di

studio e analisi, in modo da conoscere bene l'azienda, i processi, e portare l'utente ad abbassare il livello di guardia e dare inizio all'attacco. I canali possono essere diversi: mail, phone, usb. I punti deboli che possono essere sfruttati: Stabilità dei comportamenti, Validazione sociale, Liking, Sudditanza verso l'autorità vera o presunta, Reciprocità, Paura.
36) SPAM-Phishing-Mail Marketing: Pubblicizzare prodotti per fine commerciale o di phishing per portare l'utente a visitare siti falsi o pagine compromesse e catturare dati. Possono portare a danni economici o perdite di tempo. Gli Antispam possono essere: Filtri sui contenuti (probabilistici e sempre un passo indietro), Black-White listing (update delle liste, DOS per utente inconsapevoli), Greylisting (rispondere alla prima con un temporary error), Sender Policy Framework (permette controlli incrociati sugli indirizzi ip), DKIM (il mittente certifica la responsabilità di quel msg), DMARC: SPF+DKIM+ulteriori regole. Mail Marketing sono le mail non richieste. Una mail non è SPAM quando il server di invio ha una reputazione e quella mail non infastidisce il destinatario. Phishing: SPAM rivolto a rubare dati, credenziali. La difesa migliore è la consapevolezza dell'utente. Che l'utente sappia riconoscere SPAM e !SPAM. Le caratteristiche comuni: grammatica zoppicante, url accorciate, mail strane, mail invece di nomi, caratteri strani.
37) Privacy: Vi sono da considerare tre aspetti: Sicurezza (azioni fatte contro la mia volontà), Privacy (azioni che eludono la mia volontà), Reputazione online (azione fatte contro la mia volontà involontaria). Esistono 2 visioni: UK- presuppone una legittimità statale a raccogliere dati per fini amministrativi, UE- come diritto fondamentale. Le informazioni possono finire online in vario modo: Probe request degli smartphone (gestendo le reti note e risalendo l'indirizzo dell'utente), Tracciamento degli utenti tramite wifi anche indoor con precisione del metro (l'anonimato non esiste, basti pensare ai punti di interscambio), Totem pubblicitari all'ingresso (livello di soddisfazione), Fotografie (timestamp, luogo, imperfezioni del device), Google dorks (quello che sta su google lo possono vedere tutti, buoni-cattivi, con parametri speciali come: filetype, allintext, allintitle, allinurl), Mantenere online solo quello strettamente necessario e controllare tramite crawler. PYMK: algoritmo con cui META traccia le amicizie. Usa diversi pattern, alcuni: persone che si muovono insieme, nello stesso posto, imperfezioni simili nelle foto, stessa rubrica.
38) Cookie: Sono lo strumento per gestire lo stato sul web, in quanto HTTP è stateless. Possono essere: Session (relativi alla sessione del browser, si cancellano alla chiusura), Persistent (rimangono fino alla scadenza), Secure (gestiscono i login), Preferences-Statistics, 3 Parti (tracciano la navigazione dell'utente. Devono avere linguaggio semplice, possibilità di rifiuto, no al silenzio assenso, no alle cookie wall). [Third party, cookie …] Proposta alternativa sono i Topics. Permettono di fornire informazioni generiche agli inserzionisti sulla profilazione dell'utente basandosi sulla navigazione per categorie.
39) Cattivi: Esistono diverse tipologie di cattivi. Si differenziano per la complessità degli attacchi e la loro frequenza. Zona (0,1) vi sono le agenzie governative per motivi diplomatici, politici. Zona (3,7) con l'Hacktivism per motivi etici, sociali. Queste due hanno frequenza $^{1}/_{10}$. Zona (7,3) i crimini organizzati, per soldi, ransomware. Zona (1,0) con i cattivi occasionali. Poi vi sono i cattivi per conto di terzi, che vendono ad altri i servizi per attaccare. I cattivi non sono sempre perfetti, quelli isolati possono esporsi quando maneggiano i soldi. Il bersaglio spesso pensa di non esserlo, oppure può essere una sponda per attaccare altri. Gli ATT possono puntare al colpo grosso o tanti piccoli incassi. Mentre capire il nemico e identificarlo può essere complicato, soprattutto tra i non professionisti.
40) La dinamica criminale: Essa segue 5 fasi: Motivazione (quando il soggetto comincia a giustificare internamente l'idea di commettere il crimine), Fantasia criminale (quella che può rafforzare la motivazione, alimentando il desiderio di passare all'azione), Anticipazione

mentale degli effetti (qui che il soggetto decide se il crimine è fattibile e "vale il rischio".), Progettazione (il crimine passa dall'essere un'idea a un piano concreto) ed Esecuzione (quando viene effettuato. Può portare a soddisfazione, senso di colpa o ulteriore pianificazione per nascondere le tracce). L'oggetto digitale è equiparabile al bene pubblico perché non esclusivo, non rivale, e costo marginale nullo. L'analisi dei pro e contro può ridursi per il mancato contatto tra cattivo e vittima.
41) Intrusion Detection: Comprende tutte quelle attività per rilevare attività anomale sulla rete. Possono essere Network based (catturano il traffico secondo delle regole di pattern matching, lo analizzano e possono segnalare. Sono come guardiani che hanno una lista di foto dei cattivi e se ne vedono uno suonano l'allarme ma lo lasciano entrare), Host based (fanno auditing sistematico dei log e del file system, tracciano i/o. Sono come guardiani dei caveau, controllano che il dato sia ancora lì, se manca suonano l'allarme).
42) Intrusion Prevention: È un'altra attività che può essere host-network based, o con wireless system. Può comprendere blocco delle porte, del MAC address, kill dei processi, spostamento del traffico. Gestione dei log è importante per capire cosa è successo. È necessario capire per quanto tempo conservarli, se nasconderli all'utente, se proteggerli all'ATT, usare strumenti di analisi, report.
43) SIEM: Security information event management. Sono strumenti che permettono di analizzare in tempo reale gli avvisi di sicurezza generati da app o hardware in rete. Sono utili per i centri operativi di sicurezza per rilevare e rispondere a incidenti.
44) Durante gli attacchi: Le attività da effettuare: Mettere in sicurezza i dati, Conta dei danni, Pianificare il ripristino, capire come è successo. Il contrattacco è illegale. Si può avere un piano di risposta agli incidenti (che contiene i responsabili, l'elenco dei possibili rischi, le guide e le procedure. Deve essere mantenuto aggiornato e si devono fare simulazioni). Team di risposta agli incidenti che abbia competenze extra in modo che applichi decisioni strategiche. Una volta trovato il danno, si limitano i danni, si elimina la minaccia, si risana l'ambiente per tornare operativi.
45) Honeypots: Ambiente per attirare gli ATT (studiarli, distrarli). Ambiente simile a quello di produzione ma innocuo, anche per valutare attacchi in corso.
46) Sandbox: "Buca dove far esplodere gli attacchi". Dalle aziende può essere usata per eliminare programmi o codici non attendibili di terze parti senza danneggiare l'host o il OS.
47) Canary: Possono essere dei sistemi di emulazione delle reti aziendali per gestire trappole, reti fittizie e per far perdere tempo agli ATT.
48) Digital Forensics: Attività per avere delle prove valide nei processi per cybercrime. Vale il discorso di non contaminare la scena, e avere dati, prove che siano autentiche ed affidabili. L'estrazione dei dati da phone può avvenire a vari livelli: Logico (SMS, App, Contatti), File system (File, Hidden file), Fisico (Deleted data). Image forensics è l'attività sulle immagini per verificare che non siano manipolate.