La sicurezza delle informazioni attraverso la sicurezza informatica – 2a parte

Abbiamo in precedenza proposto alcune basi per un chiarimento di massima ed iniziale sull'argomento. Vediamo ora quali sono le mille domande e i mille accertamenti che ci si potrebbe porre sui due aspetti enunciati: Sicurezza della Infrastruttura Fisica e Digitale.

Sicurezza della Infrastruttura Fisica

- Come è organizzata la sicurezza perimetrale e dell'edificio: ci sono responsabili della sicurezza al cancello? È una zona recintata? la vigilanza è continua 24h al giorno? Ci sono telecamere? Sistema di videoregistrazione? Modalità di accesso alle registrazioni? Le persone sono su una lista di accesso o chiunque può entrare/accedere all'edificio? Il parcheggio esiste? Controllato? È sotterraneo o all'aperto? Esiste un posto accoglienza (reception)? Si entra con badge? il sistema è registrato? Esiste un controllo in entrata e/o uscita con scanner come negli aeroporti? Se si entra con badge, questo è valido solo per il piano interessato o i piani sono ad accesso controllato? L'accesso all'edificio è solo per dipendenti o anche visitatori? Ci sono consegne previste all'edificio/piani come ad esempio pranzo, pacchi, forniture? Se no, esiste un accesso secondario per i fornitori?
- Ci sono uffici chiusi (con vetrate o meno) o parliamo di spazi comuni e solo sale riunioni? Esiste una direttiva "NO carte" sulle scrivanie? Le scrivanie sono condivise

o personali? Parliamo di laptop o computer da scrivania? Sono protetti con cavi di sicurezza? I cassetti sono con chiave o senza? Le password sono scritte e lasciate in evidenza oppure esiste una direttiva anche per la pwd?

- La continuità elettrica è assicurata? Ci sono generatori o linea indipendente di riserva che arriva direttamente dal gestore? Se ci sono generatori esiste sicuramente una riserva di carburante: come è gestito l'accesso e la sicurezza del sito? Esiste un sistema antincendio? Che tipo di sistema: schiuma, chimico, ad acqua? Esiste una riserva d'acqua?
- Che politica esiste contro gli eventi naturali? Il sito è vicino a diga o ferrovia? Esiste la possibilità di allagamenti, frane, smottamenti, terremoti? Il sito è vicino a realtà soggette ad esplosioni e/o interesse terroristico come banche, raffinerie, industrie chimiche, depositi di esplosivi/armi? Il sito è vicino al mare e soggetto a maremoti? Il sito è un posto isolato o vicino a strade ad alto scorrimento?

Sicurezza della Infrastruttura Digitale

- I dispositivi hanno la possibilità di collegarsi a internet o solo alcuni dipartimenti ne sono collegati: commerciale, direzione etc.? Esiste una linea internet di supporto in caso di guasto (back up)? Esiste una politica riguardo la possibilità di portare e collegare il proprio laptop/smartphone/tablet al lavoro?
- La protezione perimetrale è assicurata da Firewall, Honeypot, DMZ? Ci sono sistemi di protezione con IPS e/o IDS? Gli apparati di rete (router, switch) sono configurati contro attacchi o utilizzo improprio? Esistono in atto misure di sicurezza secondo gli standard minimi di amministrazione ad esempio come port violation, ACL, port shutdown, MAC filtering, porte switch/router non collegate fisicamente e/o in shutdown amministrativo? I comportamenti anomali degli IP sono

segnalati e/o gestiti e/o bannati per indagine interna? Esistono bilanciatori per gestire il traffico in entrata e in uscita?

- I vari server sono configurati per ricevere gli aggiornamenti con le patch di sicurezza? Gli allegati alla posta aziendale sono scansionati prima della consegna agli utenti e prima della spedizione fuori dalla rete aziendale? Che livello raggiunge l'ispezione degli allegati compressi, o le macro in entrata e in uscita?
- I server antivirus gestiscono anche i dispositivi mobili, personali o meno? Esiste una politica di livello minimo di aggiornamento e/o sicurezza presenti sui dispositivi mobili, personali o meno, prima di farli accedere alla rete aziendale tipo controlli NAC? Accedono alla stessa rete aziendale di tutti i dispositivi o esiste una rete separata? La rete per gli ospiti è la stessa del personale aziendale? Quali risorse hanno a disposizione? Esiste una politica sull'uso di app consentite o meno: facebook, instagramm, google, photo e così via? Esiste un filtro per la navigazione internet con accessi e navigazione controllata e monitorata?
- Esiste un sistema di autenticazione AAA (autenticazione, autorizzazione, accounting)? Ci sono inoltre sistemi di autenticazione a più fattori e/o ad esempio retina, impronte digitali, chiavetta con sistema PIN usa e getta? Esiste un sistema per il cambio regolare e controllato delle password? Che tipo di robustezza esiste per i criteri per le password? Le politiche sono forzate o solo suggerite? Esiste una cronologia o altri criteri di osservanza quali evitare i nomi utenti, le date di nascita, e così via? Esiste una politica per le pwd anche degli apparati di rete: router, firewall, switch, servers, programmi in uso? chi e quante sono le persone autorizzate alla conoscenza delle password degli apparati di rete?

- È consentito l’uso dei floppy/cdrom/chiavette USB sui sistemi aziendali? Che tipo di protezione esiste se uno di questi dispositivi è consentito: all’avvio, all’uso, blocco in caso di ispezione sospetta?
- I desktop aziendali sono fisici o virtuali? Esiste un sistema di blocco schermata o visione impedita che non sia quella dell’utente seduto di fronte? Esiste un sistema di backup dei dispositivi consapevole o inconsapevole? Che politica è stata implementata per i backup: giornalieri, full, incrementali, differenziali, settimanali? I laptop/desktop sono collegati via rete ethernet o solo via wifi?
- Gli apparati di rete (WIFI access points) sono ad accesso controllato e/o non accessibili facilmente? La sala server è ad accesso controllato e monitorato: chiave, impronta digitale, retina, badge, registro accessi? Gli armadi di rete sono a vista o chiusi in sala server?
- I server sono virtuali o fisici? Esiste una politica di backup locale con copie reperibili in siti diversi e lontani geograficamente dal luogo di origine? Il backup è su nastro o digitale? il backup è trasferito fisicamente con mezzi propri o compagnie esterne o inoltrato su linea dedicata ad orari controllati o al momento su linee ultraveloci? Per quanto tempo è conservato il back up?
- Come avviene il disaster recevory? Che tempistica di ripristino esiste? Naturalmente se si fa parte di un CSIRT (Computer Security Incident Response Team), il tempo di risposta, Incident Response Time, deve essere estremamente basso e rapido e commisurato al danno che se ne potrebbe avere via via che il tempo passa senza servizio erogato o di risposta ad un incidente.
- Esiste una politica sul ciclo di vita delle informazioni e delle apparecchiature presenti in azienda: programmi, dati, apparati di rete, utenze, pwd, dati del personale?
- Esiste una sicurezza delle linee? Esiste una politica di

crittografia dei dati o delle comunicazioni?

Sembra che io non abbia enunciato nulla che in un buon Documento Programmatico di Sicurezza debba essere presente.

Naturalmente perché tutto funzioni bisogna che qualcuno controlli che tutto venga fatto secondo regola, quindi come norma ci dovrebbe essere anche un sistema di controllo (AUDIT), per tutto di cui sopra, con verifica dei requisiti e tempistiche di procedure. I sistemi cambiano e le persone cambiano, quindi nel processo di audit è naturalmente compreso anche una valutazione del ciclo di vita degli apparati, del software, processo ciclico di validazione dei permessi degli utenti e dei dati utente stesso

Come ultima cosa da ricordare direi che possiamo prima cercare di investigare sull'analisi del rischio:

- Quali dati si protegge? Quale servizio si eroga?
- Cosa succede se si perdono i dati o il servizio non viene erogato?
- Cosa succede se perdo un backup?

Una volta stabilità l'entità del danno possibile/probabile, si deve decidere se correre il rischio o meno e/o mettere in atto misure contingenziali. Si deve quindi decidere se investire o meno, quanto investire e quanto preparati si deve essere per fronteggiare l'accadimento di un rischio. Come si vede, una volta stabilito ciò, tutto diviene una decisione "politica/manageriale", e questo perché la sicurezza è/veniva normalmente trascurata fino al momento in cui non si subiva un danno.

Aspetto importantissimo: la formazione del personale, consapevolezza dei meccanismi d'ingegneria sociale e consapevolezza digitale, metodo di classificazione e archiviazione sono tutti aspetti che un datore dovrebbe prevedere, programmare e implementare. Il FATTORE UMANO è spesso l'anello (debole) della catena che determina la sua

forza.

L’internet delle cose, o IoT come viene indicato spesso con l’acronimo, complica le cose dal punto di vista della mole di lavoro, ma niente (o quasi) cambia dal punto di vista del principio della sicurezza: anche loro hanno un software e un IP e un ciclo di vita.

Con la massiccia introduzione di dispositivi collegati ad internet, internet non è più internet ma IoT, internet delle cose. Con una tale mole di dispositivi e informazioni che circolano su internet, i precedenti dispositivi non erano pronti e aggiornati per far fronte all’implementazione della sicurezza informatica e l’intelligenza artificiale, AI, ha fatto la sua prepotente e invadente comparsa pubblica per dare una mano.

Con l’introduzione di IoT e l’AI, la sicurezza informatica non è più tale ma Cybersecurity. Concetti vecchi, nomi nuovi per restare al passo dei tempi: IoT, Cyber (Threat, security, diplomacy, spazio, crime), NGFW e così via…

Decine e decine di riferimenti che possono fornire ulteriori spunti di conversazione e riflessione su come e cosa e quanto approfonditamente implementare le politiche di sicurezza.

Articolo a cura di **Michelangelo Stillante**

Ha una passione per il Giappone, le lingue straniere, i viaggi e la sicurezza declinata in molteplici vesti: attitudine mentale, reparti speciali, servizi segreti e informatica. Dopo 15 anni di attività tecnologica cambia vita e si unisce a Medici senza Frontiere dove ricopre vari ruoli in varie zone “calde”. Dopo 5 anni, ritorna ad una vita quasi stanziale ma sempre con MSF come ICT Infrastructure Specialist a Praga.

Tra i suoi Hobbies: lettura, scienze, viaggi, scacchi, geopolitica, arti marziali, corsa, fotografia, yoga,

subacquea.

https://www.ictsecuritymagazine.com/articoli/la-sicurezza-delle-informazioni-attraverso-la-sicurezza-informatica-2a-parte/