Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – NOVEMBRE 2020
****

Newsletter mensile con novità in materia di sicurezza delle informazioni, IT Service Management, Qualità. E' possibile dare il proprio contributo e diffonderla a chiunque.

La newsletter è inviata via MailUp, offerta da Team Quality S.r.l.

Per iscriversi, cancellarsi e leggere l'informativa privacy: http://www.cesaregallotti.it/Newsletter.html. Sulla stessa pagina è possibile consultare l'informativa sul trattamento dei dati personali.

****
Indice

****
01- Minacce e attacchi: Furto di dati a causa di un server AWS mal configurato

La notizia, dal SANS NewsBites del 10 novembre, è che sono stati violati 24,4 GB di dati relativi a ospiti di hotel a causa di un AWS S3 bucket mal configurato:
- https://www.websiteplanet.com/blog/prestige-soft-breach-report/.

Sul SANS ricordano che sono disponibili linee guida per configurare in modo sicuro i server sul cloud. Quello del CIS specifico per AWS:
- https://www.cisecurity.org/blog/cis-benchmarks-september-2020-update/.

La stessa Amazon mette a disposizione strumenti e linee guida per configurare e verificare i server:
- https://docs.aws.amazon.com/general/latest/gr/aws-security-audit-guide.html.

Non so esattamente quale errore di configurazione sia stato sfruttato, né so se è stato frutto di distrazione o di incompetenza. Vedo però che ancora molti sottovalutano l'importanza di una corretta configurazione dei server cloud. Allora è bene ripeterlo: la configurazione iniziale dei server cloud non è ottimale per la sicurezza e quindi vanno sempre previste attività di hardening e quindi chi si occupa di questi server deve avere (o acquisire) le necessarie competenze.

****

02- Multa per smantellamento scorretto di data center

Lo smantellamento scorretto di un data centre può costare caro:
- https://www.linkedin.com/posts/nicola-vanin-b03a5451_datacenter-morganstanley-rischio-activity-6720715622830944256-XjGS.

Il post non fornisce i dettagli esatti (chi ha dato la multa e quale esattamente è stata la violazione), ma sono interessanti le considerazioni: più difficile della costruzione di un data centre è il suo smantellamento perché può comportare l'interruzione imprevista di attività. Quindi, prima di procedere, è necessario inventariare correttamente le risorse e le loro dipendenze.

****

03- ENISA Threat Landscape 2020

Franco Vincenzo Ferrari di DNV GL mi ha segnalato la pubblicazione dell'ENISA Threat Landscape 2020:
- https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends?tab=publications.

Come rendere complicate le cose: bisogna iniziare a leggere "The year in review", che fornisce una guida per orientarsi tra le altre 21 pubblicazioni. La pagina delle pubblicazioni, ovviamente, non le elenca in un ordine logico, ma casuale (per esempio il "The year in review" è presentato come penultimo documento e non come primo). Non è disponibile un unico file con tutti i documenti in ordine.

A questo punto ci metterò troppo tempo a consultarlo e non so se proseguirò nella lettura. Gli altri anni avevo apprezzato il lavoro fatto e quasi sicuramente lo farei anche quest'anno, ma non sopporto questa inutile prolissità e complicazione.

****

04- MELANI Rapporto semestrale 2020/1

Melani è la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione svizzera. Ogni 6 mesi pubblica un interessantissimo rapporto con indicati eventi, minacce e raccomandazioni relativi alla sicurezza informatico. Io sono estimatore di questo rapporto che ormai da molti anni si conferma pragmatico e preciso.

E' stato pubblicato il rapporto relativo al primo semestre 2020 ed è concentrato su come l'emergenza COVID-19 sia stata sfruttata da malintenzionati:
- https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2020-1.html.

Il bello di questo rapporto è che parla anche di molto altro.

****

05- Allegati nocivi per email

Mi hanno fatto notare che gli incidenti informatici registrati dovuti ad allegati nocivi alle email hanno avuto come effetto la riconfigurazione di alcuni servizi.

Un buon esempio è la pagina di Actalis che elenca gli allegati vietati per il loro servizio PEC:
- https://www.actalis.it/news-eventi/tipi-di-file-che-non-e-possibile-allegare-ad-un-messaggio-pec.aspx.

****

06- Guida NIST per la sicurezza dello storage

Il NIST ha pubblicato la SP 800-209 "Security Guidelines for Storage Infrastructure":
- https://csrc.nist.gov/publications/detail/sp/800-209/final.

E' un documento molto tecnico, ma utile a chiunque si occupa di sicurezza. Soprattutto dovrebbe essere noto a chi amministra gli le infrastrutture di storage (anche se queste persone sembrano solitamente

disinteressate a documenti di questo tipo).

****

07- Pubblicato il Regolamento in materia di perimetro di sicurezza nazionale cibernetica

E' stato pubblicato il DPCM 131 del 2020, "Regolamento in materia di perimetro di sicurezza nazionale cibernetica", come previsto dal DL 105 del 2019. Si trova (grazie a Glauco Rampogna degli Idraulici della privacy) sulla Gazzetta Ufficiale:

- https://www.gazzettaufficiale.it/eli/id/2020/10/21/20G00150/sg.

Come per il Regolamento NIS, richiede che alcuni ministeri (e la Presidenza del Consiglio dei ministri) individuino i "soggetti inclusi nel perimetro" e che poi questi rispettino misure di sicurezza, già previste dal DL 105 del 2019 (non mi risulta siano già state pubblicate).

Non c'è molto di più in questo DPCM. Mi lascia molto perplesso l'obbligo, per i soggetti inclusi nel perimetro, di trasmettere "l'architettura e la componentistica relative ai beni ICT" alla Presidenza del Consiglio dei ministri e al Ministero dello sviluppo economico. Infatti o queste informazioni sono critiche, e pertanto non è bene che siano diffuse, oppure un po' inutili, e pertanto si sta chiedendo un inutile e costoso lavoro burocatico ai soggetti (che dovrebbero spendere soldi ed energie in altri adempimenti).

Sull'uso improprio del termine "cibernetica": sbagliare è umano, mentre la perserveranza continua a lasciarmi sbigottito.

****

08- ENISA Guidelines for Securing the IoT

ENISA ha pubblicato nuove linee guida sulla sicurezza dell'IoT dal titolo "Guidelines for Securing the Internet of Things":
- https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things.

Introduce alcuni concetti che mancavano dalla precedente "Good practices for security of IoT: Secure Software Development Lifecycle", dedicata al solo software e che segnalai a suo tempo (http://blog.cesaregallotti.it/2019/11/enisa-good-practices-for-security-of-iot.html). Questa guida tratta di tutti componenti dell'IoT, inclusi quelli fisici.

Commento: apprezzo molto questi lavori di ENISA. Purtroppo però l'organizzazione dei documenti di ENISA rende difficile capire i collegamenti tra loro e questo è un peccato.

****

09- Azure Defender for IoT

Microsoft ha pubblicato una versione per "public review" del suo nuovo prodotto agentless per la sicurezza delle reti IoT e OT:
- https://techcommunity.microsoft.com/t5/microsoft-security-and/azure-defender-for-iot-is-now-in-public-preview/ba-p/1784329.

Non faccio pubblicità a prodotti o aziende, però questo prodotto mi sembra molto interessante. Forse ne esistono di analoghi, ma finora non ne avevo incontrati. Come minimo, vanno capite le funzionalità offerte.

****

10- Il modello Emmental per valutare gli eventi

Ho trovato divertente questa vignetta che presenta il modello Emmental per la difesa da COVID-19 (i nordamericani, ahinoi, dicono "Swiss cheese"):
- https://t.co/0vFX7vaHIS.

Mi sembra una bella rappresentazione del concetto di "difesa in profondità", per cui un solo livello di

protezione non è sufficiente.

Ho poi cercato di approfondire la cosa e ho trovato questo articolo:
- https://blog.enterprisetraining.com/swiss-cheese-accident-causation-model/.

Ed ecco quali sono le lezioni che fornisce il modello Emmental:
- gli incidenti sono spesso causati dalla convergenza di più fattori;
- i fattori possono essere di molti tipi, dai comportamenti scorretti dei singoli a errori organizzativi;
- fattori molto importanti sono gli "errori latenti", che rimangono dormienti fino a quando non sono attivati da errori attivi;
- gli esseri omani sono inclini agli errori e quindi richiedono sistemi ben progettati e realizzati per prevenirli e mitigarli.

Ho letto un altro articolo dal titolo "Revisiting the Swiss cheese model of accidents":
- https://www.researchgate.net/publication/285486777_Revisiting_the_Swiss_Cheese_Model_of_Accidents.

Questo propone un'idea interessante: affinché si verifichi un incidente, devono verificarsi:
- difese inadeguate;
- comportamenti scorretti;
- precursori psicologici per i comportamenti scorretti;
- carenze organizzative (line management deficencies);
- decisioni errate della Direzione.

Sarebbero da approfondire i "precursori psicologici per i comportamenti scorretti".

Concludo sperando che qualcuno faccia (e me lo faccia vedere!) un disegno altrettanto bello di quello che ho segnalato inizialmente, ma dedicato alla sicurezza delle informazioni.

****

11- Lo stile di scrittura ISO

Sono molto attratto dalle regole di stile, non solo per ragioni professionali, ma anche per curiosità verso le regole necessarie alla nostra quotidianità (per esempio, sono un cultore de "Il saper vivere" di Donna Letizia). Quindi mi sono letto con molto piacere il "ISO house style" per la redazione degli standard:
- https://www.iso.org/ISO-house-style.html.

Al di là dei miei gusti personali, penso sia corretto usare questo riferimento per controllare meglio la scrittura dei propri documenti: uso delle maiuscole, delle abbreviazioni e degli acronimi, redazione della bibliografia, scrittura delle liste numerate e non numerate eccetera.

****

12- Imparare a imparare

Segnalo questo articolo di cui Anna Gallotti (mia sorella) è coautrice. Il titolo è "Imparare ad imparare: Fattori che permettono e facilitano il processo di apprendimento":
- http://share-coach.bmetrack.com/c/v?e=112EEA4&c=98BAC&t=0&l=3ADF5DA4&email=HuT9fCkN5V9LzXF31Fidn0kDNvJcItyC5mrjfCIPaW83Ih4P1WxctQ%3D%3D.

Credo ci siano cose molto interessanti e utili, soprattutto quando bisogna formare su qualità, sicurezza e privacy.

In particolare ho sottolineato questo passaggio: "Se è vero che ci sviluppiamo avventurandoci fuori dalla nostra zona di comfort, dovremmo stare attenti a non andare troppo oltre: l'apprendimento ottimale avviene quando ci troviamo alla giusta congiunzione tra sfida e competenza, dove non siamo appesantiti dall'ansia da una parte o dalla noia dall'altra". E quindi ripenso alle attività di formazione in cui ho fornito

troppe tracce teoriche o troppi elementi lontani dalle competenze dei partecipanti.

****

13- Privacy e EDPB: Linee guida sulla privacy by design e by default

Mi hanno segnalato la pubblicazione della versione 2.0 delle "Guidelines 4/2019 on Article 25: Data Protection by Design and by Default":
- https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en.

La lettura è molto interessante e in qualche modo riassume efficacemente molti concetti del GDPR. Però attenzione che non si tratta di una guida alle misure di sicurezza. Queste sono trattate in modo molto sommario e con un solo esempio al punto 3.8 quando parla di integrità e riservatezza.

Un'altra cosa mi ha dato da pensare ed è il suggerimento di determinare KPI per valutare l'efficacia delle misure privacy. Qui l'EDPB, purtroppo, dà ascolto ai cattedradici e promuove KPI quantitativi e qualitativi, senza però proporne di veramente significativi. Gli esempi per i quantitativi sono: percentuali di falsi positivi e falsi negativi (senza però dire di cosa), riduzione dei reclami, riduzione dei tempi di risposta agli interessati quando esercitano i propri diritti (notare che questi KPI sono dichiarati male, visto che le "riduzioni" sono obiettivi che, inoltre, oltre un certo limite, dovrebbero diventare "mantenimento"). Gli esempi per i qualitativi sono talmente generici che non aiutano molto. Però poi arriva la vera raccomandazione appropriata e applicabile: dimostrare le ragioni per cui le misure scelte si ritengono efficaci (ossia, traduco io, presentare una valutazione del rischio).

Infine: mi fa specie vedere che anche l'EDPB fa un uso inutile e scorretto di iniziali maiuscole, soprattutto quando il GDPR, da questo punto di vista, è corretto.

Comunque sia: raccomando la lettura di queste linee guida per la loro ottima sintesi (38 pagine, inclusive di copertina e indice), il rigore, la completezza e la pragmatica. Al di là delle mie insignificanti critiche, questo è un documento esemplare.

****

14- Privacy e EDPB: raccomandazioni per i trasferimenti extra SEE

L'EDPB ha messo in consultazione pubblica le raccomandazioni sui trasferimenti dei dati personali al di fuori dello SEE: "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data":
- https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en.

Innanzi tutto ricordiamoci che non è ancora un documento ufficiale, ma in consultazione pubblica.

Non tratta solo del trasferimento dei dati negli USA, ma è un'opinione più generale. E sono generali anche le raccomandazioni, tra cui quella di verificare per bene la normativa del Paese importatore, e non sono forniti strumenti semplici da consultare. Ovviamente il sogno sarebbe un sito con tutti i 200 Paesi del mondo con indicate le caratteristiche da considerare quando vi si vogliono esportare dati personali. Devo dire che siamo ancora lontanissimi da questo sogno e organi come l'EDPB dovrebbero farsi carico di queste necessità, visto che non è pensabile che migliaia di aziende (e non parlo dei DPO, le cui competenze sono troppo spesso dubbie sulle basi e quindi non possiamo aspettarci molto quando si tratta di un argomento complesso come questo) si facciano le proprie analisi di adeguatezza così come suggerite.

Grazie a Glauco Rampogna degli Idraulici della privacy per la segnalazione.

****

15- Privacy: sui cookie wall

Segnalo questo interessante video di Pietro Calorio su LinkedIn su come funzionano (male) i cookie wall:
- https://www.linkedin.com/posts/pietrocalorio_privacy-dataprotection-eprivacy-activity-6732293325866504192-j1b5.

Il video è artigianale, ma fa vedere chiaramente come sono fatti male i cookie wall. Nella migliore delle ipotesi sono estenuanti per l'utente che li rifiuta. Ne sono testimone ogni volta che vado sui siti di Amazon e molti altri perché ogni volta mi chiedono di confermare le scelte (cosa che non fanno con chi accetta i loro cookie).

****

16- Provvedimento verso l'Azienda Ospedaliera Cardarelli - Altre considerazioni

Avevo scritto sul Provvedimento verso l'AO Cardarelli:
- http://blog.cesaregallotti.it/2020/10/provvedimento-del-garante-verso.html.

Con Pierfrancesco Maistrello abbiamo ragionato ulteriormente su alcuni particolari.

Il primo riguarda la multa comminata al fornitore (ossia "responsabile", che però aveva insistito, scorrettamente, per essere identificato come titolare) di 60 mila Euro. Questa multa è più del triplo della cifra (17.135 Euro netti) con cui si era aggiudicato la gara, come ha trovato Pierfrancesco Maistrello sul portale della trasparenza dell'AO.

Quindi, sempre Pierfrancesco Maistrello, suggerisce la frase a effetto: "Se pensate di aver fatto un affare, ricordatevi che non considerare i rischi privacy vi può costare anche 3 volte quello che avete fatturato".

Inoltre conveniamo sul fatto che il ruolo di responsabile è generalmente più conveniente di un'autoinflitta titolarità.

In caso di mancata nomina (ossia di clausole contrattuali tra titolare e responsabile come da Art. 28 del GDPR), che fare? Dopo aver valutato se sia opportuno effettuare lo stesso il trattamento, è comunque opportuno ragionare operativamente "come se" si stesse operando da titolare, quindi ovviando alle mancanze del committente, soprattutto in tema di misure di sicurezza, oltre a segnalare l'anomalia al titolare vero e proprio.

Da parte mia noto che il rischio è solo citato, mentre la valutazione dell'adeguatezza delle misure segue più il principio per cui una violazione dimostra che le misure non sono adeguate. Non sembra che il Garante abbia chiesto una valutazione del rischio né che le aziende coinvolte l'abbiano presentata.

Pierfrancesco pensa che "la valutazione del rischio è un adempimento raro e la fanno solo i più virtuosi". Però, se non viene mai citata dai provvedimenti sanzionatori, almeno per segnalarne la mancanza, l'approccio basato sulla valutazione del rischio sarà ritenuto inutile. Nel Provvedimento verso Unicredit del dicembre 2018 (https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9076378) e in altri se ne fa un accenno, ma molto difficile da cogliere.

Ho guardato i recenti casi di violazione sul sito dell'EDPB e risulta solo un caso in cui l'autorità norvegese rileva che la valutazione del rischio non era stata ancora completata. Negli altri casi che ho guardato (due finlandesi e una danese), non è citata. Per contro, nel celebre caso della multa a British Airways (https://ico.org.uk/action-weve-taken/enforcement/british-airways/), mi sembra sia citata la valutazione del rischio (punto 6.22, parzialmente censurato) e quindi è chiaro che in questo caso l'approccio è considerato.

Purtroppo, infine, non sembra che vengano pubblicati i provvedimenti relativi alle violazioni ma senza sanzioni. Sarebbero interessanti per conoscere i casi positivi e poterli prendere come esempio.

****

EONL