Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – SETTEMBRE 2018

****

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

E' disponibile il blog http://blog.cesaregallotti.it.

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- DFIR for Genoa

Raccolta fondi per Genova della comunità DFIR:
- https://www.gofundme.com/dfir-for-genoa.

Mattia non è solo un amico di Genova, è un grande professionista e consiglio quanti vorrebbero "fare qualcosa" di aderire.

****

02- Corso di perfezionamento su Criminalità Informatica e investigazioni digitali

L'Università statale di Milano organizza il corso "Criminalità Informatica e investigazioni digitali":
- http://www.beccaria.unimi.it/ecm/home/didattica/corsi-di-perfezionamento/criminalita-informatica-e-investigazioni-digitali.

Lo promuovo e consiglio a tutti di partecipare (sono anche Presidente dell'associazione degli ex alunni; www.perfezionisti.it).

Scadenza 26 settembre.

****

03- Privacy: Testo consolidato del GDPR

Da un tweet dell'EDPB, il link al testo consolidato del GDPR:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504

Il testo non include i considerando. Con mia gioia, visto che non apprezzo i testi non normativi che sono però considerati "quasi normativi".

Segnalo poi che il tweet iniziava così: "Cercate una lettura per l'estate?". Mi ha divertito.

****

04- Privacy: Aggiornato il Codice privacy (D. Lgs. 101 del 2018)

Con il D. Lgs. 101 del 2018, è stato aggiornato il D. Lgs. 196 del 2003 (Codice della privacy). Il D. Lgs. 101 si trova sul sito della Gazzetta ufficiale:
- www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg.

Ringrazio una mia anonima amica per la segnalazione. Devo però dire che in questi giorni ho visto troppa fibrillazione per l'attesa di questo D. Lgs., come non vedevo neanche quelli che facevano la schedina e aspettavano i risultati delle partite. E, una volta uscita la notizia, tutti a dire quanto sono stati veloci a fornirla (come fossero dei personaggi dei film sui giornalisti). Secondo me, troppi stanno perdendo il senso del nostro mestiere.

Detto questo: il D. Lgs. 196 modificato è disponibile su Normattiva. Per chi non lo sapesse, è quello il posto giusto dove guardare:
- http://www.normattiva.it/.

Il commento di Francesco Pizzetti su Agenda Digitale mi sembra utile (ma sicuramente in futuro usciranno altri articoli; prego tutti di prestare attenzione alla reale competenza di chi li scrive):
- https://www.agendadigitale.eu/sicurezza/privacy/delega-per-il-gdpr-i-punti-forti-e-deboli-un-primo-giudizio/.

Altro articolo (molto sintetico) è di Giusella Finocchiaro:
- http://www.studiolegalefinocchiaro.it/2018/08/10/il-sole-24-ore-privacy-protetta-da-sanzioni-penali/.

Io, dopo una prima lettura, mi sono segnato alcuni punti, ma evito di trattarli nel dettaglio: altri lo faranno in modo molto più approfondito. Darò in futuro qualche link se mi sembrerà interessante. Rimane però la regola: leggere prima direttamente la normativa (il testo consolidato quando sarà disponibile) e solo successivamente gli articoli di giornale o i post sui social network.

Ecco i miei punti:

- ci sono molti aggiornamenti sui trattamenti specifici o relativi a specifici settori (ognuno deve quindi verificare quelli applicabili al proprio caso), con anche richiami sulle norme deontologiche, i minorenni;
- sono fornite le definizioni di "comunicazione" e "diffusione" (dovrò rileggere il Codice privacy e il GDPR per verificare meglio se questo ha impatto per esempio nelle informative);
- in molti casi mi pare siano promossi provvedimenti del Garante con misure prescrittive, tornando indietro rispetto all'impostazione basata sulla valutazione di adeguatezza; infatti sono stabilite regole sul mantenimento in vigore dei codici di condotta, delle prescrizioni attualmente richieste dalle autorizzazioni generali (che quindi saranno eliminate come autorizzazioni, ma rimarranno come prescrizioni), dei provvedimenti generali; è quindi necessario controllare gli aggiornamenti sul sito del Garante; questo mi induce anche a non dare per morto, tra gli altri, il Provvedimento AdS (anche se avrei voluto farlo);
- segnalo l'autorizzazione all'uso di dati biometrici per i dispositivi di controllo degli accessi, i limiti ai diritti degli interessati (per esempio, se sono in contrasto con le normative anti-riciclaggio o alla protezione delle vittime di estorsione), i diritti riguardanti le persone decedute;
- continua a sorprendermi che sia necessaria una norma per ricordare che il titolare o il responsabile (intesi come organizzazioni) possono distribuire le responsabilità all'interno dell'organizzazione stessa;
- non mi pare sia stato modificato il comma 4 dell'articolo 130, che introduce il "consenso soft"; visto che ci sono difficoltà di interpretazione su "marketing diretto per legittimo interesse e non sulla base del consenso", speravo in qualcosa di diverso;
- introdotto un articolo un po' assurdo sull'obbligo, per i fornitori di trasmissione IT (e non dei servizi più evoluti), di fornire informazioni sui rischi di violazione della sicurezza della rete; dovremo vedere come sarà attuato;
- sono introdotte, come previsto, le sanzioni penali;
- la deroga alle sanzioni è formulata in modo curioso, vago e forse inutile (visto che il GDPR fornisce dei massimi e che il Garante non è l'unico a comminare sanzioni): "Per i primi otto mesi dalla data di entrata in vigore del presente decreto, il Garante tiene conto della fase di prima applicazione delle disposizioni sanzionatorie";
- come previsto, l'allegato B con le misure minime è stato eliminato.

Relativamente alle autorizzazioni generali, il Garante ha preferito prorogare quelle esistenti per i trattamenti di dati sensibili e giudiziari (chi si occupa di privacy avrebbe già dovuto conoscerle; comunque ringrazio Pietro Calorio e Chiara Ponti degli Idraulici della privacy per aver segnalato la notizia):
- https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9026901.

Per quanto riguarda i "trattamenti specifici o relativi a specifici settori (ognuno deve quindi verificare quelli applicabili al proprio caso)", provo a farne un elenco:

- Esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (articoli 2-bis, 2-sexies, 2-quinquiesdecies; dove è specificato cos'è l'interesse pubblico rilevante per cui si possono trattare dati di categorie particolari e dove è richiesto un Provvedimento specifico del Garante);
- Minorenni (articolo 2-quinquies);
- Trattamenti di dati genetici, biometrici e relativi alla salute (articolo 2-septies, che però richiede sia preparato un Provvedimento del Garante);
- Dati relativi a condanne penali e reati (articolo 2-octies, che secondo me complica inutilmente quanto già stabilito dall'articolo 6 del GDPR);
- Ragioni di giustizia (articolo 2-duodecies);
- Persone decedute (articolo 2-terdecies);
- Forze di Polizia (abrogati, sostanzialmente, gli articoli dal 53 al 57);
- Difesa e sicurezza dello Stato (articolo 58);
- Uso dei dati pubblici (articolo 61 che richiede regole deontologiche);
- Ambito sanitario (dall'articolo 75);
- Dati relativi a studenti (articolo 96);
- Ricerca scientifica o storica o a fini statistici (articolo 97 e seguenti; articolo 104 e seguenti; è promosso un altro codice deontologico);
- Rapporto di lavoro (articoli dal 111 al 115, dove sono ribadite cose note e dove sono richieste altre regole deontologiche);
- Assicurazioni (rimane solo l'articolo 120);
- Servizi di comunicazione elettronica (articoli dal 121);
- Giornalismo, libertà di informazione e di espressione (articolo 136 e seguenti e dove sono richieste altre regole deontologiche).

Alla fine, nella maggior parte dei casi, il Codice privacy modificato non fornisce indicazioni utili e, per capire come agire da un punto di vista operativo, dovremo aspettare i provvedimenti o le regole deontologiche o i codici deontologici da parte del Garante.

Per questa veloce analisi mi sono basato sulla versione consolidata (e non ufficiale) del Codice privacy preparata da Francesco Paolo Micozzi di Array:
- https://www2.array.eu/it/nuovo-testo-codice-privacy/.

Invito a segnalarmi errori, che sicuramente ci sono, o ulteriori considerazioni di tipo "pratico".

PS: Grazie, per avermi segnalato correzioni, a Stefano Posti.

****

05- Privacy: Pubblicata la UNI/PdR 43 per la certificazione GDPR

Fabio Guasconi di Bl4ck Swan e Glauco Rampogna mi hanno segnalato la pubblicazione delle UNI/PdR 43. Come scrive Fabio: "la prima ha una valenza di linea guida; la seconda esprime requisiti che POTREBBERO costituire la base per una certificazione ex articolo 42 del GDPR".

Sono disponibili gratuitamente:
- http://store.uni.com/catalogo/index.php/uni-pdr-43-1-2018.html
- http://store.uni.com/catalogo/index.php/uni-pdr-43-2-2018.html.

Le avevo già commentate quando furono pubblicate le bozze:
- http://blog.cesaregallotti.it/2018/05/privacy-bozza-di-prassi-uni-per-la.html.

Aggiungo solo che la prima parte risulta corretta rispetto alla versione che avevo criticato. Continuo però a pensare che sia inutile alla luce di altri contributi, a mio parere più autorevoli, oggi disponibili.

****

06- Privacy: Opinioni EDPB in italiano

Sabrina Prola mi ha segnalato la pubblicazione in italiano di alcune linee guida sull'applicazione del GDPR già pubblicate in passato dal WP Art. 29 (oggi nel EDPB) in inglese.

Le linee guida sono le seguenti:
- 250 rev. 01 sulle violazioni dei dati personali;
- 251 rev. 01 sui processi decisionali automatizzati e sulla profilazione;
- 259 rev. 01 sul consenso;
- 260 rev. 01 sulla trasparenza.

Queste linee guida si trovano sul sito del Garante:
- https://www.garanteprivacy.it/web/guest/regolamentoue.

Si trovano anche sul sito dell'EDPB, con la traduzione in tutte le altre lingue:
- https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_it.

****

07- Privacy: Sentenza del TAR e competenze dei DPO

Una recente sentenza del TAR del Friuli Venezia Giulia ripropone la questione sulle competenze del DPO. Parto con il link diretto alla sentenza (grazie a Glauco Rampogna):
- https://www.giustizia-amministrativa.it/cdsintra/cdsintra/AmministrazionePortale/DocumentViewer/index.html?ddocname=5LLMWH2MBE2JVPC536FUMJHNYU&q=.

La discussione su LinkedIn è qui:
- https://www.linkedin.com/pulse/il-dpo-%C3%A8-un-professionista-del-diritto-i-diplomi-iso-balducci-romano/.

Come sempre ci sono giuristi che al termine "misure adeguate" pensano a qualche bel "protocollo", come finora hanno fatto per la 231 e per la privacy. Ci sono anche giuristi che non hanno ancora capito la differenza tra "designazione" e "autorizzazione" e "contratto". Ci sono anche giuristi che hanno inviato un "contratto di nomina a responsabile" al fornitore. E giuristi che NON rispondono agli interessati in modo chiaro, o fanno scrivere informative incomprensibili (alla faccia di quanto chiesto dal GDPR). Ci sono non-giuristi messi ugualmente male.

Detto questo, c'è chi ne sa più di me (EDPS) e ha scritto questo (grazie a Pierfrancesco Maistrello per averlo segnalato):
- https://edps.europa.eu/sites/edp/files/publication/10-10-14_dpo_standards_en.pdf.

Su LinkedIn ho letto i commenti di Riccardo Marchetti e Luca Lezzerini e concordo con loro. Riassumo: perché il DPO deve essere un giurista affiancato da tecnici e non viceversa?

Mia personale conclusione: i criteri imposti dal TAR (ossia dedurre che il DPO debba essere una persona con competenze prevalentemente giuridiche) sono buoni tanto quanto quelli originali. Solo che non è elegante che dei legali (con potere) dicono che un certo lavoro debba essere fatto da legali.

Il testo della sentenza mi ha ricordato alcune discussioni per cui c'è chi vede un conflitto di interessi tra DPO (che deve tutelare gli interessati) e il responsabile della sicurezza (che deve tutelare l'organizzazione). Non le condivido, anche perché la stessa discussione si basa sulla richiesta indipendenza del DPO. Come è noto, però, il DPO è pagato dal titolare e quindi la sua indipendenza è sempre incompleta (qui sto parlando di sostanza, nella teoria siamo tutti bravi a dire il contrario; vedo e vivo gli stessi problemi da anni con gli auditor "indipendenti").

Altri hanno commentato ricordando che il Titolare è responsabile delle proprie azioni e quindi non è compito del TAR discuterle. Condivido anche questa.

Sempre Glauco Rampogna ricorda alcuni punti: "si tenta di legittimare la separazione tra la conoscenza dell'applicazione delle misure di sicurezza e la tutela dei diritti dell'interessato, che invece il GDPR tende ad includere nel ruolo del DPO, a tutto vantaggio della parte giuridica. Il fatto poi di essere in ambito pubblico potrebbe spingere altri soggetti pubblici ad avallare questa tesi in altri ambiti, per un effetto a cascata".

Post scriptum 1
Monica Perego ha scritto a me e ad altri quanto segue. Lo sottoscrivo pienamente.
"Trattare i temi privacy significa possedere un mix di competenze organizzative, legali e tecniche. Per le ultime due puoi ricorrere ad esperti sulla base delle specifiche esigenze. La prima è più on-off. Questo si comprende molto bene quando si fa analisi dei rischi. Io in aula lavoro sulla acquisizione delle competenze organizzative. Per quello che mi riguarda il DPO deve capirne di processi e di logiche di funzionamento delle organizzazioni. Il resto se lo prende all'esterno se non lo possiede."

Post scriptum 2
Con Monica Perego avevamo pensato a come dare maggior valore legale alla richiesta della certificazione Lead auditor ISO/IEC 27001. La soluzione ce la fornisce Accredia, con la sua linea guida "I riferimenti all'accreditamento e alla certificazione nelle richieste di offerta e nei bandi di gara" (al capitolo 6 ci sono esempi pratici e Accredia usa il termine "ISMS Responsabile gruppo di audit"):
- http://www.accredia.it/news_detail.jsp?ID_NEWS=1711&areaNews=94&GTemplate=default.jsp.

Nota
Io il bando di gara oggetto della sentenza non l'ho letto. Ma mi sembra strano che la sentenza non chiarisca se il certificato LA 27001 era richiesto come sostituto di laurea.

Conclusione
Come mi ricorda Monica Perego, Antonello Soro, l'attuale Garante privacy (o, meglio, Presidente dell´Autorità Garante), è laureato in medicina (dermatologia, ma non è scritto sul sito del Garante).

****

08- Privacy: eventi e foto pubblicate

Un mio cliente vuole filmare (e poi diffondere i video) un evento con pubblico a pagamento. Come è noto ogni tanto si fanno dei primi piani dei partecipanti.

Ho chiesto ai miei contatti se potevano aiutarmi (ovviamente sapevo che la soluzione ideale è avere la liberatoria di OGNI partecipante).

Riccardo Lora degli Idraulici della privacy mi ha segnalato questo link molto utile sui casi pratici per la pubblicazione di foto degli eventi:
- http://www.fotografi.org/pubblicabilita_foto_ritratto_esempi_concreti.htm.

Pietro Calorio (sempre degli Idraulici della privacy) ha segnalato questa proposta (forse non seria) per considerare chi non vuole fornire il consenso ad essere ripreso:
- https://petapixel.com/2018/08/17/festival-dont-want-to-be-in-photos-put-a-red-dot-on-your-forehead/.

Li ringrazio molto e ringrazio anche chi vorrà fornire ulteriori approfondimenti.

****

09- Privacy: Provvedimento Garante sulla localizzazione di veicoli aziendali

Segnalo questo Provvedimento del Garante sulla localizzazione di veicoli aziendali:
- https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9023246.

In sostanza ricapitola i Provvedimenti precedenti e alcune nuove misure in relazione ai GPS sui mezzi aziendali, pertanto è utile per le aziende (e i loro fornitori!) che usano tali misure.

Il Provvedimento è stato anche pubblicizzato come "storico" perché usa per la prima volta il principio di privacy by design e privacy by default. Ritengo sia esagerato. Ma il provvedimento è comunque importante.

****

10- Privacy: Circolare dei consulenti del lavoro su come applicare il GDPR

Alla fine di questo caldo luglio italiano, il Consiglio Nazionale dell'Ordine dei Consulenti del lavoro hanno pubblicato una circolare sul "Ruolo del Consulente del Lavoro" nei termini del GDPR:
- http://www.consulentidellavoro.gov.it/index.php/component/k2/item/911-circolare-cncl-del-23-luglio-2018-n-1150.

In sostanza la circolare dice che il consulente del lavoro dovrebbe essere inteso come "contitolare" (che loro scrivono come "co-titolare").

In tanti ne hanno scritto. Io penso che il commento più in sintonia con il mio sentire l'ha scritto Davide Foresti su LinkedIn:
- https://www.linkedin.com/pulse/lordine-dei-consulenti-del-lavoro-e-il-falso-problema-davide-foresti.

Io ho avuto a che fare con consulenti del lavoro che vogliono essere titolari (e però il contratto lo hanno con l'azienda che gli trasferisce i dati personali e che pertanto deve specificare le condizioni nel contratto), altri che accettano il ruolo di responsabile (con relativo contratto). A mio avviso, purché il

contratto riporti le clausole, il resto mi ricorda il dibattito sulla natura della luce (ossia incomprensibile, se non che la soluzione è impossibile nei termini posti).

****

11- Eredità digitale: che fine fanno i dati dopo la morte

Alessandro Iocco mi ha segnalato questo articolo dal titolo "Eredità digitale: che fine fanno i dati dopo la morte":
https://inno3.it/2018/07/26/eredita-digitale-che-fine-fanno-i-dati-dopo-la-morte/.

In questi ultimi mesi ne avevo parlato con qualcuno e mi sembra un argomento da considerare. Infatti avevo assistito, a inizio 2017, ad una presentazione di Giovanni Ziccardi del suo libro "Il libro digitale dei morti", che però non ho mai letto (accipicchia!):
- http://www.utetlibri.it/libri/il-libro-digitale-dei-morti/.

Un altro articolo:
- https://www.corrierecomunicazioni.it/privacy/il-profilo-facebook-passa-agli-eredi-in-caso-di-morte-la-sentenza-storica-della-corte-tedesca/.

Il D. Lgs. 101 ha introdotto nel nostro Codice privacy proprio alcune considerazioni in merito.

****

12- Accessibilità: Ampliata la Legge accessibilità e standard EN 301 549

Non sono per niente un esperto in materia, ma credo sia importante seguirla.

E' stato pubblicato il D. Lgs. 106 del 2018 dal titolo "Riforma dell'attuazione della direttiva (UE) 2016/2102 relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici":
- www.gazzettaufficiale.it/eli/id/2018/09/11/18G00133/sg.

Modifica la Legge 4 del 2004 sull'accessibilità agli strumenti informatici da parte delle persone con disabilità. La estende ai siti web e alle applicazioni mobili degli enti pubblici.

Mi pare una bella cosa (anche se non avevo capito che la precedente Legge non includeva i siti web).

E' stato pubblicato lo standard EN 301 549 con le specifiche per l'accessibilità (da parte di invalidi) ai siti web e alle applicazioni per dispositivi mobili, con i requisiti di percezione, operatività, comprensibilità e robustezza definiti dalla Web and Mobile Accessibility Directive:
- https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=50127.

****

13- Standard: Nuova versione della ISO/IEC 20000-1

E' stata pubblicata la ISO/IEC 20000-1:2018 che sostituisce la versione del 2011:
- https://www.iso.org/standard/70636.html.

Per chi non lo sapesse, la ISO/IEC 20000-1 ha titolo "Service management system requirements" e rappresenta (mi scusino i puristi) la norma che permette di certificare l'adozione di ITIL da parte delle aziende.

Non l'ho ancora letta. So solo che è stata modificata per recepire l'HLS, ossia per essere impostata come le altre norme sui sistemi di gestione (per esempio, ISO 9001 e ISO/IEC 27001), con l'analisi del contesto, delle parti interessati, dei rischi e delle opportunità, eccetera.

****

14- Standard: Correzione alla ISO/IEC 27011

E' stata pubblicata una correzione alla ISO/IEC 27011 dal titolo "Code ofvpractice for Information security controls based on ISO/IEC 27002 for telecommunications organizations":
- https://www.iso.org/standard/76487.html.

La correzione prevede solo la modifica del titolo del paragrafo 8.2.1 da "Classification guidelines" a "Classification of information". Non molto...

La correzione è visibile direttamente dalla pagina web di iso.org attraverso la "Preview".

La ISO/IEC 27011 presenta un elenco di controlli di sicurezza per gli operatori di servizi di telecomunicazione. Questi controlli sono in realtà un'estensione di quelli della ISO/IEC 27002.

****

15- Rapporti sulla sicurezza (ENISA e CSA)

Come ogni anno, ENISA ha pubblicato la sua analisi delle minacce dal titolo "ENISA Threat landscape 2017":
- https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017.

Il periodo di riferimento è il 2017.

Le minacce considerate sono raccolte in 15 famiglie (dal malware allo spionaggio). Per ognuna sono riportate le "Specific mitigation actions", cosa decisamente interessante. Per alcune avrei sottolineato di più il ruolo dei processi e per altre avrei raccomandato misure più semplici (per esempio, per la minaccia "interni malintenzionati" avrei previsto il controllo accessi, non uno IAM).

Criticare è sempre più facile di fare. Ne sono consapevole, ma sono anche consapevole dell'elevata qualità di questa pubblicazione, che ogni anno migliora. Ne raccomando quindi la lettura.

ENISA ha pubblicato anche un rapporto relativo agli incidenti di sicurezza nel settore degli operatori delle telecomunicazioni:
- https://www.enisa.europa.eu/news/enisa-news/169-telecom-incidents-reported-extreme-weather-major-factor/.

Per i più pigri: la maggior parte degli incidenti ha come causa errori hardware o bug software, maltempo, blackout. Il 2% hanno come causa attacchi da parte di malintenzionati.

Parere personale: questo insegna anche alle imprese di altri settori che è bene non sottovalutare gli attacchi degli esterni, ma che è opportuno non dimenticare le minacce meno "di moda" ma comunque significative. Questo discorso, comunque, è vecchio e porta alla conclusione (nota da anni) che chi si occupa di sicurezza informatica deve anche occuparsi di sicurezza fisica e di manutenzione.

Franco Vincenzo Ferrari di DNV GL mi ha segnalato la pubblicazione del documento "Top Threats to Cloud Computing: Deep Dive" del Cloud Security Alliance (richiede registrazione):
- https://cloudsecurityalliance.org/media/press-releases/csa-releases-top-threats-to-cloud-computing-deep-dive/.

Si tratta di un elenco di 12 attacchi (non minacce!) particolarmente significativi e avvenuti negli ultimi anni.

Segnalo quelli per me più significativi (e, a ben vedere, non si tratta di "minacce cloud").

Il caso del 2016 di due dipendenti della società Zynga che hanno portato dati da un concorrente:
- https://arstechnica.com/tech-policy/2016/11/zynga-sues-2-former-employees-over-alleged-massive-data-heist/.

L'attacco a Yahoo! del 2013, che ha dimostrato diverse leggerezze procedurali:
- http://fortune.com/2016/12/19/yahoo-hack-cyber-security/.

****

16- Allarme sulle catene di fornitura del software

L'US National Counterintelligence and Security Center (NCSC) ha pubblicato un report dal titolo "Foreign Economic Espionage in Cyberspace". Si trova sul sito dell'NCSC:
- https://www.dni.gov/index.php/ncsc-home.

Il SANS NewsBites ne ha dato risalto fornendo un collegamento ad un articolo di infosecurity-magazine.com:
- https://www.infosecurity-magazine.com/news/us-warns-of-supply-chain-attacks/.

Non vorrei elogiarmi troppo, ma sono anni che dico che, in materia di filiere di fornitura, non bisogna prestare attenzione ai soli fornitori cloud. Ora è considerata "in crescita", ma secondo me è sempre stata troppo sottovalutata (aggiungo che dopo l'entrata in vigore del GDPR vedo maggiore attenzione nei contratti stipulati con i fornitori, mentre prima la situazione era ai confini del disastrosa).

****

17- Tecnologia e sicurezza: autenticazione a due fattori (strumenti e rischi e violazione a Reddit)

La notizia, giunta via Twitter da @skhemissa è che Reddit è stata violata da qualcuno che ha compromesso le credenziali di personale interno per accedere a dei server cloud e di immagazzinamento di codice sorgente (e quindi a dei backup di dati degli utenti in sola lettura):
- https://thehackernews.com/2018/08/hack-reddit-account.html.

La stessa notizia l'ho trovata (più sintetica) sul SANS NewsBites Vol. 20 Num. 061, che si può consultare su questa pagina:
- https://www.sans.org/newsletters/newsbites/.

Questa notizia è importante perché le credenziali erano protette da un sistema di autenticazione a due fattori (o 2-factor-authentication o 2FA) basato su SMS e questo attacco ha dimostrato che è facile comprometterlo.

Se il 2FA basato su SMS è debole, ancora più debole è il sistema basato sulle sole user-id e password (la pubblicazione NIST SP 800-63-3, che già segnalai a suo tempo, raccomandava di non usare sistemi 2FA basati su SMS).

Come consulente mi accorgo di non aver mai segnalato ai miei clienti che i servizi accessibili con sole user-id e password sono vulnerabili. Penso in particolare ai servizi su cloud (tra cui email, file sharing, backup), ma anche, ovviamente, agli altri.

La mia competenza sugli strumenti è ahimè scarsa, ma cerco di migliorarla. I meccanismi di 2FA possono essere in ordine di livello di sicurezza. Intanto rimando ad un post di Bruce Schneier di agosto 2018 che fornisce alcuni link (e in cui segnala che Google ora produce il suo token):
- https://www.schneier.com/blog/archives/2018/07/google_employee.html.

Strumenti 2FA possono essere:
- codici temporanei, o one-time, inviati via SMS (ritenuti molto insicuri, ma preferibili comunque alle sole user-id e password);
- codici temporanei inviati via app per dispositivi mobili (esempi sono Google Auth e MS Authenticator);
- chiavi USB o Bluetooth (o NFC o altro) da collegare al pc o al dispositivo mobile (esempi sono YubiKey di Yubico, U2F Security Key di Feitian e il recente Titan Key di Google, basati sul protocollo FIDO).

Prego di inviarmi ulteriori approfondimenti su questa materia.

Bruce Schneier in un altro post ha segnalato un articolo dal titolo "Before You Turn On Two-Factor Authentication…" che riporta i rischi della 2FA:
- https://medium.com/@stuartschechter/before-you-turn-on-two-factor-authentication-27148cc5b9a1.

Ci ricorda quindi che ogni misura di sicurezza porta con se dei rischi e che la sua introduzione va sempre attentamente ponderata.

Per completezza, il post di Bruce Schneier è qui:
- https://www.schneier.com/blog/archives/2018/08/good_primer_on_.html.

****

18- Tecnologia e sicurezza: IoT Devices security

Niccolò Castoldi (che ringrazio) mi ha segnalato questo documento dal titolo "CTIA Cybersecurity Certification Test Plan for IoT Devices". Il pdf si trova in questa pagina, sotto la rubrica "IoT Cybersecurity Certification Program":
- https://www.ctia.org/about-ctia/programs/certification-resources.

Il commento di Niccolò: "si tratta di una serie di controlli che la CTIA ha elaborato sulla base di molti altri standard e best practice; mi è sembrato ben fatto".

Sono d'accordo con Niccolò. Aggiungo che il documento riguarda solo i dispositivi, non anche gli altri elementi dell'architettura IoT (server o "cloud" e applicazioni per dispositivi mobili).

****

19- Tecnologia: Sulla blockchain

Avevo detto che avrei cercato di capire meglio la blockchain perché sta diventando materia per il "next big thing" con cui cercheranno di fare soldi consulenti, informatici, venditori di fuffaware, passanti e chissà chi altro.

Da un punto di vista funzionale, il concetto è abbastanza semplice: è un sistema che permette di tracciare le transazioni.

Tecnologicamente è molto complesso perché i database su cui sono tracciate le transazioni (ledger) non si trovano su un server, ma sui pc dei partecipanti. Pertanto questi database devono avere degli elevati livelli di sicurezza, tali da non permettere ai partecipanti di violarli.

Questa soluzione ha diversi problemi tecnologici (le soluzioni basate su blockchain non sono così semplici da usare, anche perché le modifiche sono molto difficili da apportare) e filosofici. Mi è piaciuto questo articolo, peraltro molto critico:
- https://medium.com/@kaistinchcombe/decentralized-and-trustless-crypto-paradise-is-actually-a-medieval-hellhole-c1ca122efdec.

Commento personale: sono molto perplesso perché quasi tutti gli articoli sulla blockchain ne promuovono la tecnologia ("la blockchain risolverà tutti i vostri problemi"), senza però indicarne i campi di applicazione, se non in modo generico.

Questo altro articolo dal titolo "When do you need blockchain? Decision models" è istruttivo:
- https://medium.com/@sbmeunier/when-do-you-need-blockchain-decision-models-a5c40e7c9ba1.

Ovviamente il primo modello è il più semplice!

Io sono uno scettico, come è noto, e quindi il modello di Lewis mi convince molto (hai un vero bisogno non ancora risolto? lo avevi risolto prima di aver sentito parlare della blockchain? allora non usare la blockchain!). Quasi tutti, comunque, dicono di non buttarsi su questa tecnologia se non quando strettamente necessario e, francamente, i casi che ho sentito finora (tracciabilità dei certificati ISO, tracciabilità del cibo, tracciabilità delle cartelle mediche, elezioni) non mi convincono.

Non sono un esperto di questa materia, né mai lo sarò (ofelè fa el tò mesté) forse questo non interessa nessuno. Però ritengo sia necessario sapere cos'è.

****

20- Tecnologia: Edge e fog computing

Tempo fa avevo scritto di fog e mist computing, dichiaranto la mia incompetenza:
- http://blog.cesaregallotti.it/2018/03/fog-e-mist-computing.html.

Franco Vincenzo Ferrari di DNV GL mi ha inoltrato questo articolo dal titolo "What Is Edge Computing?":
- https://www.cbinsights.com/research/what-is-edge-computing/.

In sostanza: con il termine "IoT" si intendono solo i sensori con limitatissime capacità computazionali (e collegati ad un server detto "cloud"); con il termine "Edge" si intendono i sensori con una capacità computazionale maggiore (o sensori collegati ad un processore "nelle vicinanze"). Questo permette di attivare elaborazioni senza transitare dal cloud.

Fin qui mi sembra tutto semplice. Solo una questione terminologica per dire cose abbastanza ovvie (a parte la tecnologia che ci sta dietro).

Poi l'articolo tira fuori il "fog computing" e io continuo a non capire di cosa si tratta.

****

21- Sicurezza: Minimum standard for improving ICT resilience

Giulio Boero mi ha segnalato il documento "Minimum standard for improving ICT resilience" dell'ufficio federale FONES della Confederazione Svizzera:
- https://www.bwl.admin.ch/bwl/en/home/themen/ikt/ikt_minimalstandard.html.

A me sembra un documento ben fatto, anche se sono sempre critico nel vedere il numero sempre più elevato di standard, linee guida, check list e simili.

Riporto quanto scritto da Giulio Boero stesso (e lo ringrazio): << il documento (corredato da relativo assessment tool in .xlsx) è prodotto dalla Confederazione Svizzera. E' abbastanza interessante (seppur non così "rivoluzionario", ma ormai c'è poco di nuovo da inventare) e presenta un approccio "elvetico" alla sicurezza informatica che può dare spunti interessanti. Il tutto mappato sui principali standard di sicurezza. >>

****

22- Guida AgID su metriche software applicativo

Franco Vincenzo Ferrari di DNV GL mi ha segnalato la "Guida tecnica all'uso di metriche per il software applicativo sviluppato per conto delle pubbliche amministrazioni" di AgID (si trova al link seguente sotto "Documentazione"):
- https://www.agid.gov.it/it/design-servizi/linee-guida-design-servizi-digitali-pa.

Mi sembra interessante ma forse (!) troppo teorico e inattuabile nella realtà.

****

23- Un breve articolo sulla assicurazioni di sicurezza IT

Breve articolo dal titolo "The rise of cybersecurity insurance":
- https://www.axios.com/cybersecurity-insurance-on-rise-companies-c2d2167e-9425-418e-bef9-6dfbc141deba.html.

Ribadisce cose già dette. L'elenco dei miei post l'avevo già fatto qui:
- http://blog.cesaregallotti.it/2016/10/assicurazioni-sulla-sicurezza-ict.html.

****

24- Commento sulle società di audit PCI

Avevo dato la notizia "Società di audit PCI citata in giudizio":
- http://blog.cesaregallotti.it/2018/07/societa-di-audit-pci-citata-in-giudizio.html.

Fabio Guasconi di Bl4ckSwan, che ringrazio, mi ha risposto come segue.

<< È tutto legato al mondo specifico che regola l'operato di una QSA company, incorniciata dalle assicurazioni specifiche ad essa richieste, dalle regole dei circuiti internazionali ivi incluse le sanzioni comminabili.

Tipicamente in caso di violazione vengono svolte delle analisi forensi dai circuiti volte ad accertare cosa è successo e se ci sono responsabilità anche dovute a negligenza / errori.

Se a valle di queste attività si scopre che il soggetto violato non aveva colpa allora non vengono erogate sanzioni e i costi di riemissione / danni legati alle carte sono gestiti dai circuiti, altrimenti tutto ricade direttamente o indirettamente sul soggetto violato.

In questo caso il soggetto violato sta dicendo che la colpa non è solo sua ma anche della QSA Company che l'ha certificato pur in presenza di una situazione non conforme, cosa che un buon QSA non dovrebbe fare né accidentalmente né tantomeno intenzionalmente. >>

****