Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS –MARZO 2020 - FORMATO #IORESTOACASA E #ANDRÀTUTTOBENE

****

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 si può consultare l'informativa sul trattamento dei dati personali.

****

Indice

****

01- Rapporti di sicurezza: Rapporto Clusit 2020

Il 17 marzo è stato pubblicato il Rapporto Clusit 2020. La pagina dove prenotarlo è:
- https://clusit.it/rapporto-clusit/.

Il rapporto è sempre interessante, anche se negli ultimi anni è sempre più apocalittico. Ne consiglio la lettura.

****

02- Rapporti di sicurezza: BCI Horizon Scan Report 2020

Il BCI ha pubblicato il rapporto "BCI Horizon Scan Report 2020" sui rischi di interruzione delle attività:
- https://www.thebci.org/resource/bci-horizon-scan-report-2020.html.

Non è relativo ai servizi informatici, ma a tutti i tipi di organizzazione.

Il primo rischio, quest'anno, è quello di pandemia, che ha superato quello di interruzione dei servizi informatici. Nulla di sorprendente... (anche se l'indagine si è conclusa a fine 2019).

****

03- ENISA e linee guida per la sicurezza negli ospedali

Mi hanno segnalato la pubblicazione di questa interessante guida dal titolo "Procurement guidelines for cybersecurity in hospitals":
- https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services.

L'ho trovata molto interessante, anche considerando che molte cose non sono applicabili solo agli ospedali ma a tutti gli ambienti "industriali".

Inoltre ho trovato interessanti la tassonomia di minacce, visto che sono 31 divise in 5 famiglie (molto maneggevoli, ma solo di tipo informatico). Accanto a queste, ho trovato utile la lettura delle sfide (challenge) e delle vulnerabilità (che indica impropriamente come "rischi").

Le misure sono un po' deludenti in quanto alcune troppo generiche, ma forse utili per alcuni lettori non troppo esperti della materia.

Segnalo la misura G 20 (Set gateways to keep legacy systems/machines connected) relativa ai dispositivi obsoleti e vulnerabili.

****

04- Tecnologia: Cifratura dei backup iPhone e Android

Da Crypto-Gram del 15 febbraio, segnalo questi due articoli sulla cifratura dei backup degli iPhone. Il primo ha titolo "Apple dropped plan for encrypting backups after FBI complained":
- https://www.reuters.com/article/us-apple-fbi-icloud-exclusive-idUSKBN1ZK1CT.

Il secondo ha titolo "Apple may have ditched encrypted backups, but Google hasn't":
- https://www.androidcentral.com/apple-may-have-ditched-encrypted-backups-google-hasnt.

Mi pare che i titoli dicano già tutto sulla questione della cifratura dei backup degli smartphone. Io sono sempre stato restio a fare i backup del mio cellulare (anche per la ridotta quantità di dati), ma a questo punto riconsidererò la cosa per l'Android.

****

05- Poster dell'NSA sulla sicurezza (anni 50 e 60)

Da Crypto-gram del 15 febbraio, segnalo i "NSA Security Awareness Posters":
- https://www.schneier.com/blog/archives/2020/01/nsa_security_aw.html.

Sono 136 poster. Alcuni sono un po' datati, ma altri sono decisamente interessanti.

****

06- Compromissione delle password dei dispositivi IoT

Da Crypto-Gram del 15 febbraio 2020 segnalo questo articolo dal titolo "Half a Million IoT Device Passwords Published":
- https://www.zdnet.com/article/hacker-leaks-passwords-for-more-than-500000-servers-routers-and-iot-devices/.

Un hacker ha pubblicato le password di accesso a mezzo milione di dispositivi accessibili via Telnet e con password o di fabbrica (quindi mai cambiate dall'utilizzatore) o molto semplici.

Tutto questo dimostra, ancora una volta, come questi dispositivi sono progettati e sviluppati, visto che fanno uso di protocolli da tempo considerati insicuri e non prevedono procedure affinché gli utenti li installino in modo sicuro senza fatica.

****

07- Cultura e gestione: Successo e insuccesso

Mia sorella scrive di coaching e non sempre riesco a capire l'ambito del suo lavoro. Però molte cose di cui scrive mi incuriosiscono. Questa volta segnalo quindi un articolo di Anna Gallotti e Selika Cerofolini dal titolo "2020: è tempo per una nuova definizione di successo". Credo che non sia pubblicato da qualche parte pubblica.

Provo a mandare questi due link:
- prima parte:
http://share-coach.benchurl.com/c/v?e=F8AD48&c=98BAC&t=0&l=3ADF5DA4&email=HuT9fCkN5V9LzXF31Fidn0kDNvJcItyC5mrjfCIPaW83Ih4P1WxctQ%3D%3D;
- seconda parte:http://share-coach.benchurl.com/c/v?e=FD7327&c=98BAC&t=0&l=3ADF5DA4&email=HuT9fCkN5V9LzXF31Fidn0kDNvJcItyC5mrjfCIPaW83Ih4P1WxctQ%3D%3D.

Innanzi tutto bisogna considerare che il successo è un mito moderno. Viviamo nell'"illusione della meritocrazia", per citare il filosofo Alain de Botton, dove non solo riteniamo che le possibilità di scalare la vetta siano infinite, ma anche che, poiché è possibile, dobbiamo farlo, nel modo in cui ci dicono di farlo.

Però nessuno può avere successo in tutto, e sicuramente non sempre, indipendentemente da ciò che ci dicono. Il tempo per la famiglia paga spesso il prezzo di una carriera brillante ad esempio, ed è difficile essere popolari mantenendo una incrollabile integrità. La buona notizia è che possiamo scegliere quali sono le nostre priorità.

L'articolo dice altre cose interessanti. Per quanto riguarda gli argomenti di cui mi occupo, possiamo trarre questa sintetica lezione (se già non l'avessimo presa da altre parti): non si può avere la sicurezza perfetta, la qualità perfetta, la privacy perfetta, eccetera. Dobbiamo toglierci queste illusioni e decidere quali sono le priorità.

****

08- Mio articolo sull'accreditamento

E' stato pubblicato questo mio articolo dal titolo "Accreditamento e certificazioni: regole, metodologie e norme di riferimento":
- https://www.cybersecurity360.it/legal/accreditamento-e-certificazioni-regole-metodologie-e-norme-di-riferimento/.

Mi ha chiesto un po' di lavoro di studio, visto che volevo essere sicuro dei tipi di accreditamento di cui volevo scrivere.

Mi spiace che nei ringraziamenti non appaia Stefano Ramacciotti insieme a Franco Ferrari e Alice Ravizza. Purtroppo per colpa mia e per la mia fretta di inviare l'articolo (anche se quelli di Cybersecurity 360 potrebbero correggerlo senza fatica).

****

09- Articolo sull'accreditamento dei laboratori di VA

Appena pubblicato il mio articolo sull'accreditamento, Paolo Sferlazza di Gerico mi ha segnalato un suo articolo dal titolo "L'accreditamento dei laboratori che effettuano Vulnerabily Assessment":
- https://www.ictsecuritymagazine.com/articoli/laccreditamento-dei-laboratori-che-effettuano-vulnerabily-assessment/.

Mi pare un ottimo approfondimento su questo tipo di accreditamento.

****

10- Conservazione dei documenti informatici, cloud e blockchain

Segnalo questo articolo di Andrea Lisi di ANORC dal titolo "La conservazione dei documenti informatici non si fa in cloud o in blockchain":
- https://anorc.eu/attivita/la-conservazione-dei-documenti-informatici-non-si-fa-in-cloud-o-in-blockchain/.

Il titolo dice già tutto e quindi non commento ulteriormente, ma ne raccomando la lettura.

****

11- Standard: Traduzione in italiano della ISO 22301

E' stata pubblicata la ISO 22301:2019 in italiano. Come spesso succede, visto che il recepimento come norma UNI e la traduzione sono successive al recepimento come norma europea (EN), la norma prende nome UNI EN ISO 22301:2019:
- http://store.uni.com/catalogo/uni-en-iso-22301-2019.

****

12- Standard: Nuova versione della ISO/IEC 27002 sugli audit agli ISMS

Franco Vincenzo Ferrari di DNV GL Business Assuranche mi ha segnalato la pubblicazione della ISO/IEC 27007:2020 dal titolo "Guidelines for information security management systems auditing":
- https://www.iso.org/standard/77802.html.

Non grandi cambiamenti rispetto alla precedente versione, a parte l'allineamento alla ISO 19011:2018, di cui scrissi a suo tempo:
- http://blog.cesaregallotti.it/2018/07/nuova-iso-190112018-guida-per-laudit.html.

****

13- Cybersecurity Maturity Model Certification (CMMC)

Avevo già incontrato il CMMC durante la lavorazione del libro sull'IoT che sarà presentato al prossimo Security summit (o chissà quando, visto il corona-panico). Franco Vincenzo Ferrari di DNV GL Business Assurance mi ha poi inoltrato un link interessante.

Ma andiamo con ordine. Il primo link che propongo è quello dal titolo "Understanding Cybersecurity Maturity Model Certification (CMMC)":
- https://www.securityorb.com/featured/understanding-cybersecurity-maturity-model-certification-cmmc/.

Qui capisco quanto segue:
- chi vorrà lavorare con il DoD degli USA dovrà conseguire questa certificazione;
- la certificazione è basata su 5 livelli;
- a gennaio era prevista la pubblicazione del materiale anche a scopo di formazione.

Il secondo articolo (grazie a Franco) ha titolo "Cybersecurity Maturity Model Certification (CMMC) Levels" e presenta più dettagli:
- https://securityboulevard.com/2020/01/cybersecurity-maturity-model-certification-cmmc-levels/.

Il terzo URL (grazie ancora a Franco) è quello delle FAQ ufficiali:
- https://www.acq.osd.mil/cmmc/faq.html.

Quindi gli USA stanno producendo il loro schema proprietario di sicurezza informatica, promuovendo ulteriormente schemi in contrasto con quelli ISO o simili. Chi non ha poteri politici, come me, potrà solo guardare come la situazione si evolverà.

****

14- Privacy: Sanzione del Garante in ambito sanitario

Mi hanno segnalato questo interessante provvedimento del Garante privacy "Ordinanza ingiunzione nei confronti di Azienda Ospedaliero Universitaria Integrata di Verona" del 23 gennaio 2020 (doc web 9269629):
- https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9269629.

Qui trovo interessante la prima osservazione del Garante (punto 6, primo elemento dell'elenco puntato). La traduco: "vi multo perché avete dimostrato di non aver adottato misure idonee, visto che sin dal 2013 vi dicevo di attuare le misure che, mancando, vi hanno portato ad una violazione di dati personali".

Traduco ulteriormente: meglio seguire le misure segnalate dal Garante.

****

15- Privacy: Garante, Aruba e la gestione delle prime password e delle credenziali amministrative

Questo Provvedimento del Garante mi piace un sacco (non per Aruba, ma per il contenuto tecnico, ovviamente):
- https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9283040.

Da una verifica al servizio PEC di Aruba a seguito di alcune segnalazioni di violazioni, il Garante ha identificato 3 criticità:
- al momento dell'assegnazione iniziale della password ai titolari delle caselle di posta, non veniva richiesta la modifica obbligatoria con anche criteri di lunghezza e complessità (questo fino al 25 settembre 2019);
- accesso ai log da Internet di persone che usavano credenziali condivise (e di tipo amministrativo);
- memorizzazione, all'interno dei file di log applicativi, di troppi dati (incluse username e password riportate in chiaro).

Immagino tutti sappiano che queste sono criticità, ma tanti di noi sanno che spesso non sono affrontate per mille motivi (soprattutto di carico di lavoro e perché, ahinoi, inizialmente il servizio non è stato progettato pensando a questo aspetto). Ora il Garante ribadisce che vanno corrette. Non ha dato alcuna multa, ma spero che questo sia sufficiente per tutti.

****

16- Privacy: Sistema di gestione e Gdpr: integrare Mop e Mog

Segnalo questo articolo dal titolo "Sistema di gestione e Gdpr: integrare due modelli (Mop e Mog) per evitare sanzioni":
- https://www.agendadigitale.eu/sicurezza/privacy/sistema-di-gestione-e-gdpr-integrare-due-modelli-mop-e-mog-per-evitare-sanzioni/.

L'hanno scritto due persone che stimo molto e che propongono sempre idee molto interessanti.

****

17- Pubblicazioni su pandemia, COVID-19 e smart working

Sono uscite molte cose su pandemia e COVID-19. Ovviamente è come chiudere il cancello dopo che i buoi sono scappati. Però io ho avuto l'occasione di studiare un po' di cose. Segnalo le cose per me più interessanti.

"Pandemic Planning and Implementation for Business Resiliency" dal BCI e scritta da Laura Zarrillo (che ho il piacere di conoscere personalmente). Una breve pubblicazione con molte indicazioni interessanti:
- https://www.thebci.org/news/coronavirus-pandemic-planning-and-implementation-for-business-resiliency.html.

Puntata del 2 marzo di IusLaw WebRadio dal titolo "Tutto sullo smart working":
- https://webradioiuslaw.it/speciale-adeguamento-privacy-tutto-sullo-smart-working/.

Articolo "Smart working, come garantire sicurezza informatica e privacy" (degli stessi partecipanti alla trasmissione radio di cui sopra):
- https://www.agendadigitale.eu/sicurezza/smart-working-come-garantire-sicurezza-informatica-e-privacy/.

Aggiungo che, quando si parla di smart working, mi piacerebbe approfondire anche le tematiche non di sicurezza, visto che lo strumento può introdurre inefficienze e problemi, che poi si riversano sulla sicurezza. Esempi che mi vengono in mente: come assicurare la presenza di un ambiente "alienante" (ossia che produce ricchezza ai partecipanti grazie alla presenza degli "altri", al contrario degli ambienti "estranianti"), come evitare il senso di solitudine, come educare al movimento fisico.

Manuale dell'Ufficio federale della sanità pubblica della Confederazione Svizzera (lo trovo molto buono e ringrazio Guido Uglietti per la segnalazione):
- https://www.bag.admin.ch/bag/it/home/krankheiten/ausbrueche-epidemien-pandemien/pandemievorbereitung/pandemiehandbuch.html.

****

18- Corona virus: Solidarietà digitale

Lo Studio legale Stefanelli & Stefanelli mette a disposizione dei documenti standard, predisposti dai professionisti dello studio, soprattutto relativi alla privacy, utili per riorganizzare i processi interni in questo momento di emergenza per il COVID-19:
- https://www.studiolegalestefanelli.it/it.

Iniziativa lodevole. Io adotto uno stile meno formale, ma ho apprezzato molto i modelli predisposti.

****

19- Si fa presto a dire "smart working"

Da milanese, sono interessato ad alcune cose sul corona virus. Una di queste riguarda il consiglio di attivare il lavoro da casa. Sono numerosi gli
articoli e gli interventi che, in sintesi, dicono di pensare alla continuità operativa e di attivare lo smart working. Alcuni più prolissi, altri più sintetici, ma trovo pochi approfondimenti (ho già consigliato una buona pubblicazione svizzera poco tempo fa).

Nella mia vita lavorativa e in questi giorni ho però raccolto alcune indicazioni per cui dire "lavoro da casa" (o, "lavoro agile" o, in inglese, "smart working", anche se non sempre è agile - ci si alza meno dalla sedia e qualcuno ne ha sentito la fatica -, non sempre è da casa e non sempre è furbo) non è così semplice.

Prima: molti contratti non lo prevedono. E allora ringrazio la circolare di Borioli & Colombo che mi ha segnalato il fatto che sono state attivate misure provvisorie per accedere a questo strumento. Ecco il link:
- https://www.lavoro.gov.it/strumenti-e-servizi/smart-working/Pagine/default.aspx.

Interessante ricordarsi dei rischi e la circolare segnala il sito dell'INAIL (che,

colpevolmente, non conoscevo per niente):
- https://www.inail.it/cs/internet/attivita/prevenzione-e-sicurezza/conoscere-il-rischio.html.

Seconda: non tutti hanno il pc portatile aziendale; non tutti quelli che ce l'hanno se l'erano portato via il venerdì sera. Ancora peggio: alcuni non hanno proprio un pc in casa (né quello aziendale). E altri ancora non hanno connessioni sufficienti per il telelavoro. Bisognava preventivamente fare un censimento della strumentazione che la persona metterebbe a disposizione e SE è disponibile a farlo. Sono questioni non semplici, su cui alcuni ci stanno lavorando da anni per trovare la giusta quadra tra le esigenze aziendali e quelle dei lavoratori.

Terza: se è richiesto il BYOD con strumenti di emergenza (ossia il pc personale che fino a ieri non era previsto fosse usato per ragioni di lavoro), come configurare questi strumenti? Come la singola persona può installarsi il software per la VPN o il software necessario? E si ricorda tutte le password? Come sopra, questo doveva essere pianificato preventivamente. Devo dire che ho visto aziende molto organizzate per questo tipo di situazione, ma la maggior parte non lo è.

Quarta: se è tutto a posto, l'organizzazione ha la capacità per sostenere tutto il traffico, che prima era interno, da Internet e sulle VPN?

Quinta: ora che la riunione non la facciamo più in una sala riunioni in azienda, riusciremo a farla ognuno in casa propria e con i bambini a casa da scuola?

Ripeto: queste sono questioni che ho visto direttamente e che mi sono state poste da alcuni clienti nel corso degli anni. Sicuramente ce ne sono altre e sarebbe interessante raccoglierle in modo da migliorare le nostre competenze.

Alla fine di questo elenco di possibili problemi, devo dire che molti hanno attivato il "lavoro da casa" con successo e quindi forse alcuni miei dubbi non sono così significativi.

****

20- Corona virus e privacy

Lo confesso... non ce l'ho fatta e ho risposto su LinkedIn a questo articolo dal titolo "Tutelare la privacy sui luoghi di lavoro ai tempi del coronavirus: ecco come":
- https://www.cybersecurity360.it/news/tutelare-la-privacy-sui-luoghi-di-lavoro-ai-tempi-del-coronavirus-ecco-come/.

Purtroppo ho risposto malamente anche ad uno come Luca Bolognini, da cui dovrei solo imparare.E però volevo avere un'occasione per allegare la foto che segue. Non riesco a risalire all'autore, ma spero accetti questa diffusione.

Comunque... come descritto dall'articolo, alcune aziende mandano questionari ai dipendenti, collaboratori e visitatori per chiedere se sono stati in Cina o Codogno o se

sentono i sintomi del corona virus. Alcuni consulenti privacy si chiedono quanto tempo conservare questi dati e come fare l'informativa.

La risposta è già nella domanda: il trattamento è completamente inutile e proprio per questo non è possibile stabilire i tempi di conservazione dei dati e come fare l'informativa.

Una risposta più tecnica è che, per il principio di minimizzazione, meglio sarebbe non raccogliere proprio i questionari, visto che ci sono strade alternative. Ossia informare bene le persone e dire loro cosa devono fare. Fare un bello schema, magari ispirandosi alle FAQ del Ministero della salute: http://www.salute.gov.it/portale/nuovocoronavirus/dettaglioFaqNuovoCoronavirus.jsp?lingua=italiano&id=228.

Viene da chiedersi come possa essere venuto in mente alle aziende di raccogliere i dati per proteggere il proprio personale. Infatti saprebbero interpretare le risposte? Se uno dice di essere stato a Codogno, sanno cosa fare? E allora perché chiederlo a tutti e non dire semplicemente cosa devono fare quelli che sono stati a Codogno? E poi, come interpretare i sintomi?

Purtroppo alcuni pensano di fare la cosa "giusta" (e soprattutto coprirsi le spalle) inviando questionari e raccogliendo dati, senza chiedersi cosa farsene veramente e senza fare reale informazione. La burocrazia inutile, purtroppo, sembra sempre una buona soluzione, ma non lo è.

Alcuni si sono lamentati perché il Garante non si pronuncia. Ma il Garante non è competente per dire cosa fare in caso di emergenza in sanità. Quindi non sa dire se è necessario per le aziende raccogliere i dati delle persone (visitatori e dipendenti e simili) per tutelare le aziende. Quindi: prima l'autorità competente (Ministero della salute? Protezione civile? non lo so perché su questo sono assolutamente impreparato) deve dire quali misure intraprendere, poi (o consultanto preventivamente) il Garante dirà la sua nel caso in cui queste misure includano il trattamento dei dati personali.

Se consultato preventivamente, immagino chiederà (come dovremmo fare noi consulenti privacy) se è proprio necessario raccogliere i dati personali o non ci sono altre strade per ottenere gli stessi (o forse migliori) risultati.

PS: qualcuno mi ha detto che dovrei essere meno "massimalista". Sono comunque pronto a sapere se ci sono eccezioni da cosiderare (ossia aziende che devono necessariamente raccogliere dati personali per il corona virus e non possono seguire strade alternative).

****

#AndràTuttoBene

EONL