Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – GIUGNO 2019

****

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- Minacce e attacchi: Caso pratico di phishing di successo: i 15 milioni di Tecnimont.

Fabrizio Monteleone di DNV GL mi ha segnalato questo articolo dal titolo "Truffa del Ceo alla Tecnimont: falsa mail del capo fa partire un bonifico da 18 milioni di dollari":
- https://milano.fanpage.it/truffa-del-ceo-alla-tecnimont-falsa-mail-del-capo-fa-partire-un-bonifico-da-18-milioni-di-dollari/.

Il caso di phishing mirato (o "truffa del CEO") è da manuale e vale la pena ricordarla come caso di studio. Non è la prima (ne ho trovate altre con una semplice ricerca su Qwant) e per questo andrebbe usata come esempio per tutti.

****

02- Minacce e attacchi: Topi e indisponibilità

Sandro Sanna mi ha segnalato questa notizia dal titolo "Topi rosicchiano la fibra, mezza provincia di Belluno rimane senza web":
https://www.ilmattino.it/napoli/cronaca/topi_fibra_provincia_senza_web_belluno_oggi_ultime_notizie-4536425.html

Non un notizione, ma ci ricorda di controllare, nell'ambito della manutenzione, la derattizzazione (che può anche prevedere l'uso di vernici particolari sui cavi). Anche questa è sicurezza delle informazioni...

****

03- Normativa: Pubblicato il Cybersecurity Act

Franco Vincenzo Ferrari di DNV GL mi ha segnalato la pubblicazione del Cybersecurity Act sulla Gazzetta ufficiale dell'Unione europea.

Ora l'atto in italiano si chiama ufficialmente "Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»)" ed è scaricabile da qui:
- https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32019R0881.

Hanno tradotto con il brutto termine "cibersicurezza" e non con il termine sbagliato di "sicurezza cibernetica". C'è speranza.

Qualche mese fa avevo già segnalato un articolo (che usa malamente il termine "cibernetico" e non approfondisce gli schemi di certificazione dei prodotti):
- https://www.agendadigitale.eu/sicurezza/cybersecurity-act-ecco-cosa-ci-aspetta-dopo-la-direttiva-nis/.

Avevo anche segnalato il comunicato stampa del Consiglio della UE, con alcuni punti significativi del provvedimento:
- https://www.consilium.europa.eu/it/press/press-releases/2018/12/19/eu-to-become-more-cyber-proof-as-council-backs-deal-on-common-certification-and-beefed-up-agency/.

****

04- Normativa: PSD2

Un articolo di ictBusiness.it mi ha ricordato l'importanza che la Direttiva sui servizi di pagamento potrebbe avere. Infatti, tra le altre cose, è richiesto ai negozi virtuali di prevedere l'autenticazione forte dei clienti. L'articolo di ictBusiness.it si concentra su questo aspetto e sul fatto che ancora molte imprese sono in ritardo con gli adeguamenti dei propri siti di e-commerce:
- http://www.ictbusiness.it/cont/news/acquisti-online-aziende-europee-in-ritardo-sulle-nuove-norme/43134/1.html.

La PSD2 ha ulteriori impatti. A questo proposito ho trovato questo articolo su Agenda Digitale molto completo (anche troppo, per le mie competenze):
- https://www.agendadigitale.eu/cittadinanza-digitale/pagamenti-digitali/psd2-quello-ce-sapere-norme-interchange-fee-sicurezza/.

****

05- NIST Secure Software Development Framework (SSDF)

Il NIST ha pubblicato la bozza di un documento dal titolo "White Paper: Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)":
- https://csrc.nist.gov/publications/detail/white-paper/2019/06/11/mitigating-risk-of-software-vulnerabilities-with-ssdf/draft.

Temevo fosse il solito documento "fai valutazione del rischio e arrangiati (noi autori, in realtà, non sappiamo niente di tecnologia, ma possiamo scrivere tomi sulla valutazione del rischio e sui processi)". Invece ho trovato alcuni elementi interessanti, anche se non c'è tantissima tecnologia. la sintesi aiuta.

In bibliografia ho trovato il riferimento ad un documento dal titolo "Fundamental Practices for Secure Software Development: Essential Elements of a Secure Development Life Cycle Program":
- https://safecode.org/news/safecode-publishes-fundamental-practices-secure-software-development-essential-elements-secure-development-life-cycle-program/.

Un altro documento abbastanza breve (38 pagine), in cui mi pare ci siano consigli pratici che non trovo facilmente in giro.

E questo documento mi ha fornito il link al "SEI CERT Coding Standards":
- https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards.

Penso non ci siano scuse per chi scrive in C, C++, Java, Perl e Android.

Se posso segnalare dei difetti: i siti, alla fine, si concentrano soprattutto sulla parte di codifica e poco sulla parte funzionale e su quella architetturale.

****

06- ENISA Industry 4.0 - Cybersecurity Challenges and Recommendations

Sandro Sanna mi ha segnalato la pubblicazione del breve (13 pagine) studio di ENISA dal titolo "Industry 4.0 - Cybersecurity Challenges and Recommendations":
- https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations.

Le raccomandazioni (riassunte da me) sono:
- allineare le competenze in materia di IT e OT (segnalo che è scritto che le persone in ambito OT devono adattarsi alle innovazioni, me, ma non è esplicitato che gli "esperti" di IT devono capire le caratteristiche dell'OT, per esempio in termini di sicurezza delle persone e lunghezza del ciclo di vita dei prodotti);
- prestare attenzione alle regole stabilite (solitamente incomplete) e alla necessità di fornire fondi alla sicurezza;
- incoraggiare con incentivi la sicurezza;
- prestare attenzione ai prodotti per industria 4.0 perché il loro ciclo di vita è la composizione di quello dei prodotti IT e OT;
- chiarire le responsabilità tra gli attori di industria 4.0;
- prestare attenzione al fatto che gli standard in materia di industria 4.0 sono frammentati;
- gestire la sicurezza considerando tutta la filiera di fornitura;
- prestare attenzione all'interoperabilità e alla sicurezza dei prodotti industria 4.0.

****

07- Mio articolo su ITIL 4

E' stato pubblicato su ICT Security magazine il mio articolo dal titolo "ITIL 4 Foundation":
- https://www.ictsecuritymagazine.com/articoli/itil-4-foundation/.

Nulla in più di quanto avevo già scritto sul blog.

****

08- Plugin QWAC per Firefox

Glauco Rampogna (professionista della sicurezza delle informazioni e della privacy) mi ha segnalato che AgID ha pubblicato un plug-in per Firefox per validare i Qualified Website Authentication Certificates (QWAC):
https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2019/05/31/The+Agency+for+Digital+Italy+brings+online+security+to+the+next+level.

Il nome divertente (QWAC) vuol dire che per Regolamento (e non per fiducia "nel sistema") è possibile validare i certificati SSL di un sito web.

Glauco ha commentato: "per una volta pare che siamo i primi".

Per il resto, io ho installato il plug-in e prossimamente vedrò come lavora.

****

09- Privacy: VERA per privacy - versione gamma

Ho aggiornato il VERA per privacy, usando i controlli della ISO/IEC 27552 al posto di quelli della ISO/IEC 29151.

Infatti la ISO/IEC 29151 è per soli titolari, mentre la ISO/IEC 27552 è rivolta a titolari e responsabili, oltre ad essere meglio organizzata, grazie anche alle esperienze accumulate nei 2 anni di utilizzo.

La ISO/IEC 27552 è al momento in fase di final draft, però i controlli finali saranno quelli (al limite mi sono sbagliato con la numerazione).

Per la versione GAMMA, grazie a: Nicola Nuti, Simona Persi, Chiara Ponti.

Il VERA 4.4 privacy GAMMA è scaricabile da qui:
- http://www.cesaregallotti.it/Pubblicazioni.html.

Dopo l'estate vorrei creare un VERA 5.0 per privacy e per 27001 (vorrei cercare di fare un unico file, in modo che uno lo possa usare per la sola ISO/IEC 27001, la sola privacy o per tutte e due contemporaneamente). Quindi: chiunque ha suggerimenti è pregato di farmeli avere.

PS: sono consapevole che "versione gamma" non è mai usata (a meno di eccezioni che non conosco), ma dopo la versione beta ho trovato questa soluzione.

****

10- Privacy: Mio articolo sulla ISO/IEC 27552 sui sistemi di gestione privacy

Segnalo la pubblicazione del mio articolo "Gestione dei dati personali, ecco le novità della norma ISO/IEC 27552":
- https://www.agendadigitale.eu/sicurezza/privacy/gestione-dei-dati-personali-ecco-le-novita-della-norma-iso-iec-27552/.

Devo dire che, rileggendolo, non mi sembra scritto bene. Spero che almeno sia chiaro.

****

11- Privacy: GDPR e questioni aperte

Segnalo questo interessante articolo di Agenda Digitale dal titolo "GDPR, i rinvii alla Corte di Giustizia Ue: i principali nodi da sciogliere":
- https://www.agendadigitale.eu/sicurezza/privacy/gdpr-i-rinvii-alla-corte-di-giustizia-ue-i-principali-nodi-da-sciogliere/.

L'articolo elenca i casi ora in esame presso la Corte di Giustizia UE. Questi, pertanto, ci forniscono alcune indicazioni su alcuni dubbi interpretativi e su cosa ci potrebbe aspettare in futuro.

****

12- Privacy: GDPR: la crittografia non basta

Segnalo questo breve articolo di Alessandro Vallega dal titolo "GDPR e sicurezza, vogliamo dirci la verità? L'encryption non basta":
- https://www.cybersecurity360.it/soluzioni-aziendali/gdpr-e-sicurezza-vogliamo-dirci-la-verita-lencryption-non-basta/.

In poche e buone parole dice quello che emerge da questi 12 mesi di attuazione del GDRP: per pigrizia e incompetenza, in tanti richiedono l'applicazione della crittografia (in modo generico, senza indicare né come né dove) solo perché citata (non richiesta obbligatoriamente!) dal GDPR, senza pensare ad altre misure probabilmente prioritarie.

Sebbene conosca personalmente Alessandro, ho avuto notizia di questo articolo dalla newsletter del Clusit del 31 maggio 2019.

****

13- Privacy: Garante e formazione gratuita per DPO

Il Garante ha lanciato il progetto T4DATA, ossia eventi di formazione gratuita per DPO del settore pubblico e privato.

Il primo evento sarà ad Ancona il 7 giugno e poi ce ne saranno altri. Sono anche previsti webinar:
- https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9113500.

Provvedo a diffondere la notizia, anche perché l'iniziativa mi sembra molto meritoria.

****

14- Privacy: Manuale sul diritto europeo in materia di protezione dei dati - ed. 2018

Nicola Nuti degli Idraulici della Privacy e Franco Vincenzo Ferrari di DNV GL mi hanno segnalato la pubblicazione del "Manuale sul diritto europeo in materia di protezione dei dati - edizione 2018" da parte del Council of Europe:
- https://publications.europa.eu/en/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1/language-it.

****