Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – NOVEMBRE 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- Tecnologia della sicurezza: Studio ENISA su Industria 4.0
02- Standardizzazione: Mio articolo sulla nuova ISO/IEC 27005 "Information security risk management"
03- Minacce e attacchi: Violazione delle PEC
04- Minacce e attacchi: Come spiare la CIA? Usando Google
05- Minacce e attacchi: Attacchi ai fornitori di software
06- Le password peggiori del 2017
07- Privacy: Elenco del Garante dei trattamenti che necessitano di PIA
08- Configurare i browser per la privacy
09- Accredia e i laboratori di vulnerability assessment
10- Come diffondiamo le nostre informazioni

****

01- Tecnologia della sicurezza: Studio ENISA su Industria 4.0

ENISA ha pubblicato uno studio dal titolo "Good Practices for Security of Internet of Things in the context of Smart Manufacturing":
- https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot.

La lettura è decisamente interessante anche se, a mio parere, il documento poteva essere più sintetico. Rimane una lettura molto consigliata, non solo per chi si occupa di IoT o di Industria.

****

02- Standardizzazione: Mio articolo sulla nuova ISO/IEC 27005 "Information security risk management"

Segnalo questo mio articolo dal titolo "Nuova edizione della ISO/IEC 27005 "Information security risk management":
- https://www.ictsecuritymagazine.com/articoli/nuova-edizione-della-iso-iec-27005-information-security-risk-management/.

****

03- Minacce e attacchi: Violazione delle PEC

Riporto da Wired una notizia dal titolo "Un attacco hacker ha violato 500mila caselle pec in Italia":
- https://www.wired.it/internet/web/2018/11/20/italia-attacco-hacker-account-mail-pec/.

Su ICT Business è detto che l'attacco è iniziato il 12 novembre:
http://www.ictbusiness.it/cont/news/attacco-alla-pec-italiana-colpite-500mila-caselle/42536/1.html.

Altro articolo del 15 novembre (letto su Twitter, da @Il_Vitruviano):
- http://www.dagospia.com/rubrica-29/cronache/hacker-all-rsquo-assalto-tribunali-interrotti-servizi-informatici-187938.htm.

Il nostro "vice direttore per la cybersecurity del Dipartimento delle informazioni per la sicurezza (Dis)" Roberto Baldoni suggerisce di cambiare la password della nostra PEC, ma questo è un consiglio che tecnicamente non mi pare significativo: se il mio provider di PEC non è stato compromesso (sembra sia stato compromesso quello di TIM), perché dovrei cambiare la password?

E poi ancora: se è vero che l'attacco non era molto raffinato, quali vulnerabilità sono state sfruttate?

****

04- Minacce e attacchi: Come spiare la CIA? Usando Google

Questo articolo di cui dà notizia il Sans NewsBites (l'avevo già visto su Twitter, ma in un momento di pigrizia) ha titolo "How did Iran find CIA spies? They Googled it":
- https://arstechnica.com/tech-policy/2018/11/how-did-iran-find-cia-spies-they-googled-it/.

In sostanza e se ho capito correttamente, dopo aver scoperto inizialmente come gli agenti della CIA comunicavano tra loro usando certi siti web, gli iraniani riuscivano a seguire le comunicazioni semplicemente usando Google.

Ancora una volta questo dimostra quanto siamo inconsapevoli della potenza delle tecnologie che usiamo e sarebbe quindi opportuno smettere di essere così ingenui.

****

05- Minacce e attacchi: Attacchi ai fornitori di software

Dal SANS NewsBites del 26 ottobre, segnalo la notizia dal titolo "Two New Developer Supply Chain Attacks":
- https://www.sans.org/newsletters/newsbites/xx/85#2.

Sono due attacchi a software open source: i malintenzionati hanno modificato parti del codice. La cosa è ovviamente inquietante e mi pare sia difficile trovare contromisure (a meno di non promuovere il software proprietario, che però ha altri problemi).

Questa notizia me ne ricorda un'altra relativa alla filiera di fornitura IT: quella per cui alcuni microchip, prodotti in Cina, sono stati alterati inserendo dei dispositivi di intercettazione. Si trova nel numero precedente del SANS Newsbites:
- https://www.sans.org/newsletters/newsbites/xx/84.

La notizia originale era stata data da Bloomberg, ma molti pensano sia un falso (tra l'altro per rinforzare la voglia di autarchia dimostrata da parte degli statunitensi). Visto che ha fatto notizia, la segnalo:
- https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

****

06- Le password peggiori del 2017

Come ogni anno, Splashdata pubblica le password peggiori:
https://www.teamsid.com/worst-passwords-2017-full-list/.

Lettura divertente, non troppo originale, ma da conoscere.

****

07- Privacy: Elenco del Garante dei trattamenti che necessitano di PIA

L'11 ottobre il Garante italiano ha pubblicato l'elenco dei trattamenti che necessitano di PIA:
- https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9058979.

L'elenco recepisce i commenti dell'EDPB del 26 settembre.

Non mi pare introduca trattamenti imprevisti. Alcuni però li trovo scritti in modo lievemente ambiguo e secondo me in alcuni casi si scateneranno dei dibattiti.

L'elenco fa spesso riferimento alla linea guida WP 248. Si può trovare in questa pagina (per l'italiano è necessario aprire lo zip cliccando su "Available language versions"):
- https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

****

08- Configurare i browser per la privacy

Dal Sans NewsBites del 7 novembre, ecco un articolo dal titolo "How to Lock Down What Websites Can Access on Your Computer":
- https://www.wired.com/story/how-to-lock-down-websites-permissions-access-webcam/.

La cosa interessante, come fa notare un commento del SANS, è che oggi o browser sono così complessi che hanno delle funzionalità per configurare delle funzionalità e che molto spesso poi queste cambiano, rendendo difficile la rincorsa.

****

09- Accredia e i laboratori di vulnerability assessment

Accredia ha lanciato un servizio di accreditamento dei laboratori di vulnerability assessment rispetto alla ISO/IEC 17025 (grazie a Franco Vincenzo Ferrari di DNV GL per la segnalazione):
- https://www.accredia.it/servizio-accreditato/vulnerability-assessment/.

I laboratori possono essere certificati ISO 9001 o ISO/IEC 27001, ma possono anche essere direttamente accreditati dall'Organismo di accreditamento, che in Italia è Accredia.

L'esigenza viene principalmente dall'attuazione italiana del Regolamento eIDAS e di altri servizi fiduciari quali per esempio quelli relativi alla conservazione dei documenti. Come troppo spesso succede, AgID e Accredia hanno voluto essere più bravi di quelli bravi e imporre l'uso di laboratori accreditati per l'esecuzione di vulnerability assessment presso i fornitori di servizi fiduciari.

Potevano ovviamente richiedere, ai fornitori di servizi di vulnerability assessment, le "sole" certificazioni ISO 9001 o ISO/IEC 27001. Invece hanno voluto richiedere l'accreditamento come laboratori.

Vedremo come sarà recepito questo nuovo schema, gestito direttamente da Accredia.

****

10- Come diffondiamo le nostre informazioni

Segnalo questo tweet:
- https://twitter.com/stefanoepifani/status/1058700175634513921.

Ho notato in questi mesi quanto le persone siano paranoiche nella vita "reale" (io a scuola andavo da solo da quando ho 7 anni e Milano non era più sicura negli anni Settanta - Ottanta) e invece poco attente nella vita "social-virtuale" (confesso che aspetto con sempre maggiore impazienza la notizia di qualche furto in casa di quelli che si sentono in dovere di segnalare sempre dove sono).

A parte le mie considerazioni personali, è necessario ricordare come la cultura quotidiana ha poi impatti nella sicurezza delle informazioni.

****