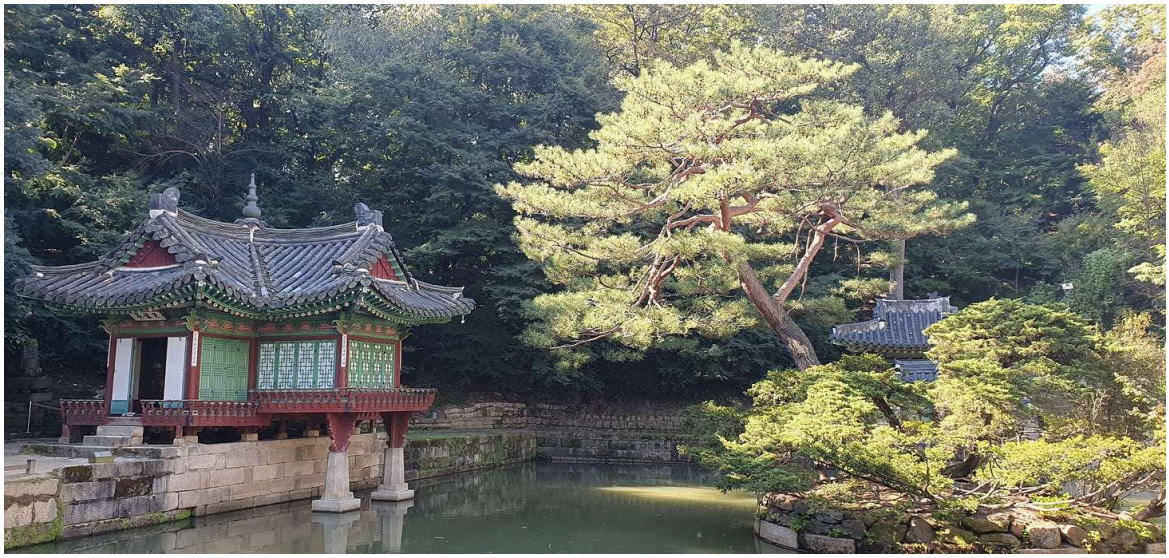
Infosec & Quality [ITA] - Ott. 2023

23 Oct 2023



Secret garden del Changdeokgung (Seoul). Ottobre 2023. Foto mia.

Indice

14- Minacce e attacchi: ENISA Cybersecurity Threat Landscape 2023

15- Minacce e attacchi: Aumento delle campagne RAT

16- Rilevare i testi generati dall'IA

17- Gli uomini possono fare tutto (Ottobre 2023)

****

01- Standardizzazione: Stato delle norme ISO/IEC 270xx - ISMS

Il 20 ottobre si è concluso il meeting semestrale dei WG 1 (dedicato ai sistemi di gestione per la sicurezza delle informazioni o ISMS) e WG 5 (dedicato alla privacy) del ISO/IEC JTC 1 SC 27.

In questo articolo riporto le attività del WG 1 che ritengo più significative.

Sono partiti i lavori per l'aggiornamento della ISO/IEC 27000 (Panoramica dei sistemi di gestione per la sicurezza delle informazioni), della ISO/IEC 27003 (linee guida per l'implementazione di un ISMS), ISO/IEC 27008 (linee guida per la valutazione dei controlli di sicurezza delle informazioni), ISO/IEC 27109 sull'istruzione e la formazione sulla cibersicurezza.

Stanno continuando i lavori per la ISO/IEC 27017 (estensione dei controlli della ISO/IEC 27002 ai servizi cloud, importante per le molte certificazioni ISO/IEC 27001 che la usano come estensione) per allineare la versione attuale con i controlli della ISO/IEC 27002:2022. Immagino che la nuova norma sarà pubblicata a fine 2024.

Sarà pubblicato a breve un aggiornamento della ISO/IEC 27006-1 (norme per l'accreditamento degli organismi di certificazione) e poi ripartiranno ancora i lavori per "pulirla" dai riferimenti scorretti a requisiti e controlli, ricordando che i controlli non sono requisiti e nessuno di essi va pianificato e implementato come da norma, ma usato solo come riferimento per la Dichiarazione di applicabilità.

Sarà pubblicata a breve la ISO/IEC 27011 (estensione dei controlli della ISO/IEC 27002 per il settore delle telecomunicazioni). La ISO/IEC 27013 (relazioni tra ISO/IEC 27001 e ISO/IEC 20000-1) e la ISO/IEC 27019 (estensione dei controlli della ISO/IEC 27002 per il settore dell'energia) sono in uno stadio precedente e saranno probabilmente pubblicate a metà 2024.

Riflessioni sono state fatte sul fatto che la prossima versione della ISO/IEC 27001 dovrà avere requisiti sui cambiamenti climatici a causa dei cambiamenti apportati all'HLS (o Annex SL, ossia la struttura base che devono rispettare tutti gli standard per i sistemi di gestione). Ci si è chiesto quali impatti sui cambiamenti climatici possono essere considerati per un sistema di gestione per la sicurezza delle informazioni.

****

02- Standardizzazione: Stato delle norme ISO/IEC 270xx - Privacy

Il 20 ottobre si è concluso il meeting semestrale dei WG 1 (dedicato ai sistemi di gestione per la sicurezza delle informazioni o ISMS) e WG 5 (dedicato alla privacy) del ISO/IEC JTC 1 SC 27.

In questo articolo riporto le attività del WG 5 che ritengo più significative.

Ho seguito i lavori sulla ISO/IEC 27701, per i sistemi di gestione per la privacy (Privacy information management system, PIMS). Era prevista per metà 2024 la pubblicazione di un aggiornamento limitato al riallineamento dei controlli con quelli della ISO/IEC 27002:2022. L'ISO Central Secretariat ha invece chiesto di ristrutturare lo standard come gli altri sui sistemi di gestione. Tutti gli esperti hanno concordato sulla necessità di ristrutturarlo completamente e, quindi, ritardare la pubblicazione per evitare incoerenze ed errori (qualcuno auspica la pubblicazione per inizio 2025, io penso che ci vorrà più tempo).

Sarà pubblicata entro metà 2024 una nuova versione della ISO/IEC 27006-2 (per gli organismi di certificazione), ma sarà necessario rifare tutto per rendere questo standard compatibile con la futura ISO/IEC 27701. Il rischio è di essere rapidi nella pubblicazione dei criteri di certificazione (la futura ISO/IEC 27701), ma più lenti per i criteri di accreditamento (la futura ISO/IEC 27006-2, sempre se manterrà questa numerazione); in altre parole, potremmo avere una nuova versione della ISO/IEC 27701, ma nessun organismo di certificazione che può condurre audit e rilasciare certificati per mancanza di regole appropriate.

Stanno continuando i lavori per la ISO/IEC 27018 (estensione dei controlli della ISO/IEC 27002 per la privacy dei servizi cloud, importante per le molte certificazioni ISO/IEC 27001 che la usano come estensione) per allineare la versione attuale con i controlli della ISO/IEC 27002:2022. Si prevede di pubblicarne l'aggiornamento a metà 2024 (ma mi sembra una data troppo ottimistica e io prevedo fine 2024).

Segnalo che si discute anche della ISO/IEC 29151 (i lavori di aggiornamento sono appena partiti). Questa norma è destinata ai soli titolari del trattamento e riprende i controlli della ISO/IEC 27002, ne estende le linee guida per l'implementazione e ne aggiunge altri specifici per la privacy. Mi sembra che in Italia sia completamente ignorata, mentre in altri Paesi è usata come riferimento dalle PMI che non intendono usare la ISO/IEC 27701 (anche se poi, una veloce ricerca online mi dice che Huawei Cloud, non certo una PMI, è "certificata" rispetto a questa norma che, tra l'altro, non prevede uno schema certificazione). Si prevede di pubblicarne l'aggiornamento a fine 2025.

****

03- Guida CISA su Identity and Access Management

Dal SANS NewsBites del 6 ottobre 2023, segnalo la notizia "CISA and NSA: Identity and Access Management Guidance", che a sua volta rimanda alla pubblicazione "Identity and Access Management: Developer and Vendor Challenges".

Questa pubblicazione non mi è sembrata molto interessante perché riassume alcune criticità, peraltro note.

C'è però un riferimento a un altro documento di marzo 2023 dal titolo "Identity and Access Management: Recommended Best Practices for Administrators": https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3336001/esf-partners-nsa-and-cisa-release-identity-and-access-management-recommended-be/.

Questo, anche se non dice nulla di nuovo, mi sembra più interessante per un bel ripasso delle regole base per il controllo accessi. Da segnalare che gran parte del documento è dedicato alla promozione di tecniche MFA.

****

04- Security-by-Design and Default Principles del CISA - Aggiornamento

Ad aprile avevo segnalato l'ottimo documento del CISA (Cybersecurity & infrastructure security agency degli USA) dal titolo "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default". E' stato aggiornato con maggiori dettagli per dimostrare il rispetto dei tre principi: https://www.cisa.gov/resources-tools/resources/secure-by-design.

In realtà non è più disponibile la versione precedente, quindi non so indicare con precisione i cambiamenti. In aprile avevo detto che "in poche pagine (15 in tutto, incluso indice e fuffa introduttiva) sono riportati e spiegati i principi di sviluppo e ingegnerizzazione sicuri". Ora le pagine sono 36, ma credo che i dettagli in più aiutino e non appesantiscono.

****

05- I più comuni errori di configurazione delle reti IT (e le mitigazioni)

Dal SANS NewsBites del 6 ottobre 2023, segnalo la notizia "CISA and NSA: Most Common Network Misconfigurations", che a sua volta fa riferimento al documento "NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations": https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a.

Il pdf si trova al seguente link: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3549369/nsa-and-cisa-advise-on-top-ten-cybersecurity-misconfigurations/.

Nulla di nuovo, certamente, ma sempre utile da ripassare.

Segnalo che da pagina 17 a pagina 27 si trovano le raccomandazioni per gli utilizzatori, da pagina 27 a pagina 31 si trovano le raccomandazioni per gli sviluppatori di software.

Insomma: si tratta di un manuale tecnico estremamente utile.

****

06- C'è carenza di esperti di sicurezza informatica (o di cibersicurezza)?

Da Crypto-gram di ottobre 2023 segnalo "On the Cybersecurity Jobs Shortage": https://www.schneier.com/blog/archives/2023/09/on-the-cybersecurity-jobs-shortage.html.

Molti si lamentano della carenza di persone competenti nell'ambito della sicurezza informatica (o cibersicurezza o cybersecurity). Bruce Schneier riporta un commento di Ben Rothke. In sostanza dice che molti ruoli sono specialistici, non generalistici. Ed è vero che c'è carenza di persone con competenze specialistiche ed è ancora più difficile trovarle se pensiamo che per avere competenze specialistiche è necessario avere anche esperienza.

Aggiungo che, almeno in Italia, ci sono difficoltà a trovare persone per ricoprire certi ruoli, anche generalisti.

****

07- Quaderno Clusit "Certificazioni professionali in sicurezza informatica 3.0"

È stato pubblicato un nuovo quaderno Clusit intitolato "Certificazioni professionali in sicurezza informatica 3.0". Sono uno degli autori, insieme da Fabio Guasconi e Federico Gozzi.

Il quaderno è liberamente scaricabile in formato pdf da https://clusit.it/blog/quaderni-clusit-certificazioni-professionali-in-sicurezza-informatica-3-0-giugno-2023/.

Riporto di seguito la presentazione del Clusit.

Si tratta di un aggiornamento e revisione dei quaderni pubblicati nel 2005 e nel 2013 da Clusit sullo stesso tema.

Nel quaderno sono descritte certificazioni che dimostrano competenze tecnologiche accanto a quelle che dimostrano competenze principalmente organizzative. In questa edizione abbiamo preferito non riportare le certificazioni relative a prodotti specifici, essendo queste troppo numerose.

Si è cercato di schematizzare il più possibile le specifiche di ogni certificazione, in modo da aiutare coloro che selezionano il personale o scrivono bandi di gara a stabilire quali certificazioni corrispondono alle caratteristiche richieste e nel contempo i professionisti che vogliono certificare e far riconoscere le proprie competenze in un determinato settore ed essere inseriti in una comunità di professioniste e professionisti con cui scambiare competenze ed esperienze.

****

08- European Cybersecurity Skills Framework (ECSF)

Franco Vincenzo Ferrari mi ha segnalato la pubblicazione del European Cybersecurity Skills Framework (ECSF) di ENISA: https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework.

La pagina segnalata permette poi di scaricare l'ECSF Role Profiles document, dove sono specificati i 12 profili tipici per la cibersicurezza. Come sappiamo, questi possono essere utili per condividere la terminologia usata per le qualificazioni professionali.

Mi sono chiesto come si correlasse con la UNI 11621-4, aggiornata al 2020 e con titolo "Profili di ruolo professionale relativi alla sicurezza delle informazioni". Ho rivolto la domanda a Fabio Guasconi, che mi ha risposto che il lavoro di ENISA è stato strutturato allo stesso modo, ha profili praticamente uguali a quelli della UNI 11621-4, con alcune differenze nella scelta delle competenze e abilità (skill).

Io noto che la norma italiana fa riferimento alla sicurezza delle informazioni, mentre quella ENISA alla cybersecurity e immagino che questo abbia i suoi, seppur marginali, risvolti.

Temo la confusione che si potrebbe creare. Vedremo.

****

09- Formazione gratuita sulla sicurezza online per cittadini, imprese e Istituzioni

Il Comune di Milano (dove risiedo) promuove il portale web Cyber Secure City:

https://cybersecurecity.it/.

Il portale, che non richiede neanche registrazione, mette a disposizione materiale di formazione gratuito sulla sicurezza informatica.

Sono presenti percorsi per Over 65, Studenti e tutti i cittadini e corsi in lingue diverse dall'italiano.

Iniziativa lodevole (e, in milanese, piutost che nient, l'è mei piutost) però i percorsi non sono progettati con cura: sembrano più una raccolta di materiale messo a disposizione, sempre lodevolmente, da alcune aziende, senza un vero filo conduttore.

Altro problema è che alcune istituzioni, piuttosto che organizzare incontri, rimandano a questo sito. Invece gli incontri e i confronti sono fondamentali per una migliore consapevolezza.

****

10- Nuova versione della NIST SP 800-82 sull'OT

Segnalo la pubblicazione della r3 della NIST SP 800-82 dal titolo "Guide to Operational Technology (OT) Security": https://csrc.nist.gov/pubs/sp/800/82/r3/final.

Io avevo letto la versione 2 e l'avevo trovata molto interessante. Riporta molte cose che si ritrovano nelle IEC 62443, ma in formato gratuito.

I cambiamenti apportati da questa versione 3 sono numerosi e sono riassunti nell'ultima pagina. Non riesco al momento a rileggere tutto il documento.

Noto però che il NIST sta proseguendo nella sua campagna di "de-sintetizzazione" e infatti questa versione è di 316 pagine, mentre la precedente era di 247 (più del 20% in più).

****

11- Nuovo Regolamento macchine e cybersecurity

E' stato pubblicato il Regolamento (UE) 2023/1230 relativo alle macchine. Esso abroga la Direttiva macchine, ossia la Direttiva relativa alla sicurezza delle macchine industriali (questa mia indicazione è molto imprecisa e serve solo a contestualizzare).

Su questo argomento ho letto con interesse l'articolo "Il nuovo Regolamento Macchine: la Cybersecurity Industrial elemento essenziale dal Design della Macchina e durante tutto il suo ciclo di vita": https://www.ictsecuritymagazine.com/articoli/il-nuovo-regolamento-macchine-la-cybersecurity-industrial-elemento-essenziale-dal-design-della-macchina-e-durante-tutto-il-suo-ciclo-di-vita/.

In pochissime parole, il Regolamento introduce in modo molto chiaro la necessità di valutare la sicurezza delle macchine anche relativamente all'hardware e al software. Questo è molto giusto perché hardware e software che non funzionano correttamente possono portare a funzionamenti imprevisti e, quindi, pericoli per le persone.

Il testo del Regolamento si trova qui: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32023R1230.

Il regolamento si applicherà dal 14 gennaio 2027.

Ancora una volta, i dettagli su come valutare le macchine saranno ulteriormente specificate nella normativa di armonizzazione.

****

12- Data Governance Act ora applicativo: così cambia l'economia digitale

Segnalo questo articolo dal titolo "Data Governance Act ora applicativo: così cambia l'economia digitale": https://www.agendadigitale.eu/sicurezza/privacy/la-data-economy-alla-prova-del-data-governance-act-lo-scenario/.

Non credo che mi occuperò mai di DGA, ma credo sia comunque opportuno sapere che esiste.

****

13- Digital Security Festival (17-27 ottobre 2023)

Luca Moroni mi ha segnalato il Digital Security Festival, che si tiene, con partecipazione gratuita, dal 17 al 27 ottobre in Veneto e Friuli Venezia Giulia: https://www.digitalsecurityfestival.it.

I temi sono tanti e interessanti. Luca, a sua volta, parlerà il 26 ottobre pomeriggio a Vicenza in una tavola rotonda dal titolo "Rischi, opportunità e futuro della cybersecurity".

****

14- Minacce e attacchi: ENISA Cybersecurity Threat Landscape 2023

ENISA ha pubblicato il Cybersecurity Threat Landscape 2023: https://www.enisa.europa.eu/news/eu-elections-at-risk-with-rise-of-ai-enabled-information-manipulation.

L'attenzione di ENISA si rivolge soprattutto su: campagne di manipolazione di informazioni (fake news), social engineering verso persone specifiche, trojan in pacchetti software noti (che si scaricano da siti ovviamente contraffatti per trarre in inganno le persone), sfruttamento degli errori di configurazione dei sistemi, delle reti e dei servizi cloud.

Le prime minacce (manipolazione di informazioni e social engineering) sono sempre più efficaci grazie all'uso di strumenti basati sull'intelligenza artificiale, che permettono di applicare vecchie tecniche, ma in modo più efficiente ed efficace.

Io qui ho evidenziato alcune cose dell'Executive summary, ma il documento è più ampio.

Purtroppo la parte relativa alle misure di mitigazione è estremamente sintetica e non aggiunge nulla di significativo (è principalmente un elenco di controlli ISO/IEC 27002 e NIST CSF).

****

15- Minacce e attacchi: Aumento delle campagne RAT

Il titolo può far ridere se non si sa che RAT vuol dire "Remote access trojan". Le campagne sono sempre più numerose e il CERT AgID spesso le segnala via Telegram o Twitter (ora X).

Segnalo uno degli ultimi avvisi dal titolo "Sempre più preoccupante il fenomeno delle campagne RAT": https://cert-agid.gov.it/news/sempre-piu-preoccupante-il-fenomeno-delle-campagne-rat/. Interessante è leggere come il RAT si diffonde, ossia con campagne di phishing ben congegnate. In questo caso, è inviato un pdf via email dicendo che si tratta di una fattura non pagata; l'utente la apre e si avvia un programma che scarica e installa il RAT.

Le comunicazioni mi sembrano molto ben fatte e interessanti, ma mancano due righe sulle strategie di mitigazione.

****

16- Rilevare i testi generati dall'IA

Da Crypto-gram di ottobre 2023, segnalo l'articolo "Detecting AI-Generated Text": https://www.schneier.com/blog/archives/2023/09/detecting-ai-generated-text.html.

Versione breve: non sembra si possano avere strumenti per rilevare automaticamente un testo generato dall'IA.

Un commento (ironico, mi pare...) fa notare che forse questa stessa risposta è stata generata dall'IA.

****

17- Gli uomini possono fare tutto (Ottobre 2023)

Quest'estate mia moglie ha dovuto seguire un corso di formazione. Con i bambini (o ragazzi) sono andato al mare per 5 giorni in un appartamento. Abbiamo tenuto ordinato e pulito, abbiamo cucinato, ci siamo tenuti ordinati e puliti.

Mi hanno dato del "mammo" e me ne sono lamentato: il termine "mammo" fa sembrare che certe cose possano farle solo le mamme e i papà le debbano fare solo in casi straordinari. Io ho cercato di fare il papà (forse malamente, ma questa è un'altra storia).

****

EONL