Infosec & Quality [ITA] - Lug. 2023

24 Jul 2023

Levanzo. Luglio 2023. Foto mia.

Indice

****

00- Editoriale

Come sempre, la newsletter a luglio esce un po' tardi e ad agosto se ne sta in vacanza. Ci risentiamo a settembre.

Faccio a tutti gli auguri di una buona estate.

****

01- 18 settembre: Convegno su NIS2 e non solo

Io sono membro del direttivo dell'associazione DFA. Abbiamo organizzato un incontro perché negli ultimi anni sono state pubblicate numerose normative dedicate alla sicurezza dei sistemi informatici e delle reti in Italia e in Unione Europea e il numero e la complessità di queste normative ci hanno posto numerosi interrogativi e li vorremmo affrontare, evidenziandone gli aspetti pratici da affrontare e raccogliendo le esperienze già fatte.

L'incontro ha nome DFA Open day e sarà il 18 settembre 2023 a Milano (all'Università Statale di Milano).

Si parlerà di:

- Ambito di applicazione e relazioni tra le normative e ruolo delle autorità di controllo;
- Rischi cyber e come valutarli e affrontarli per rispondere alle normative;
- Gestione degli incidenti e delle notifiche, considerando i diversi ambiti di applicazione delle normative, le diverse autorità da coinvolgere e le diverse regole da seguire;
- Sistemi di certificazione, in particolare quelli che saranno promossi da ACN e ENISA;
- Accordi di condivisione delle informazioni sulla cybersicurezza.

Locandina e link per registrarsi e partecipare (gratuitamente): https://perfezionisti.it/events/open-day-2023/.

****

02- Morto Kevin Mitnick

E' morto Kevin Mitnick, uno degli hacker più abili. Non un grande tecnico, ma uno con la capacità di inventare tecniche per ingannare le persone e spingerle a svelare password e altri segreti.

Consiglio a chiunque si occupa di sicurezza di leggere il suo primo libro, "L'arte dell'inganno": https://www.feltrinellieditore.it/opera/larte-dellinganno-1-2/. Anche se è del 2002, quindi con riferimenti tecnologici obsoleti, è ancora fondamentale proprio perché la tecnologia non è così importante.

La notizia l'ho appresa da Not Boring Privacy:
https://www.instagram.com/p/Cu6GaqXtYnj/?igshid=MTc4MmM1YmI2Ng.

****

03- Enisa - Good Practices for Supply Chain Cybersecurity

Davide Giribaldi di Swiss Cyber Com mi ha segnalato la guida di Enisa dal titolo "Good Practices for Supply Chain Cybersecurity" e uscita a fine maggio:
https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity.

Riporto le considerazioni di Davide, che ringrazio:

"La Guida è riferita solo all'analisi degli operatori essenziali (che poi non si chiameranno più così per la NIS2) e importanti.

La mia impressione è che evidenzi un aspetto interessante, ovvero la difficoltà non tecnica, ma organizzativa e culturale alla responsabilizzazione delle terze parti. (Fig. 6 pag. 12 del report) dove la certificazione di uno standard (ISO/IEC 27001 ad esempio) viene visto come elemento di garanzia (corretto se si esce dalla logica nota a tutti che spesso, per le PMI, le certificazioni sono pezzi di carta necessari e non una vera e propria filosofia su cui basare la strategia aziendale), ma allo stesso tempo evidenzia difficoltà ad adottare criteri come quello dell'audit sul campo nei confronti dei fornitori.

Molto interessante anche il risultato della verifica sui criteri aziendali considerati per la valutazione dei rischi informatici della catena di fornitura. Tra questi segnalo la "spesa" fatta nei confronti del fornitore, considerato il terzo più importante.

Sia chiaro, più spendo nei confronti di un fornitore, più mi fido dei suoi prodotti e servizi, ma non credo sia un elemento oggettivo di cybersecurity".

****

04- Questionario Clusit per la sicurezza dei fornitori

Il Clusit ha pubblicato un questionario per la selezione di fornitori ICT:
https://clusit.it/blog/questionario-per-la-sicurezza-dei-fornitori/.

L'idea è quella di proporre un questionario di riferimento per tutte le organizzazioni che vogliono analizzare i propri fornitori (potenziali e attivi). in merito alla sicurezza informatica.

Questo dovrebbe evitare il proliferare di questionari che, soprattutto ad alcune aziende, richiede troppo lavoro inutile, visto che si assomigliano tutti, ma sono diversi e ciascuno richiede tempo per essere analizzato e per scrivere le risposte.

Applaudo quindi all'iniziativa e la raccomando a tutti.

****

05- Sentenza sull'uso di Dropbox da parte dei dipendenti

Segnalo questo articolo dal titolo "Accesso abusivo a sistema informatico o telematico da parte di dipendenti o collaboratori": https://www.altalex.com/documents/2023/07/05/accesso-abusivo-sistema-informatico-telematico-parte-dipendenti-collaboratori.

In pochissime parole (se ho capito giusto): un dipendente aveva aperto una cartella Dropbox (pubblica!) per scambiare i dati aziendali con clienti e colleghi; poi si licenzia e cambia le credenziali alla cartella in modo che l'azienda non possa più accedervi. Alla fine viene ritenuto colpevole.

A questo proposito è ovvio che è discutibile il fatto che l'azienda abbia permesso al dipendente di aprire una cartella non controllata dall'azienda stessa su un sistema di file sharing pubblico. Vanno però anche ricordate le questioni relative alla "proprietà" della cartella: se è usata per l'azienda, sembra che debba rimanere di "proprietà" dell'azienda.

****

06- INAD, Indice Nazionale dei Domicili Digitali

Segnalo questo comunicato di AgID dal titolo "Nasce INAD, l'Indice Nazionale dei Domicili Digitali": https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2023/06/06/nasce-inad-lindice-nazionale-domicili-digitali.

Non sono uno che aderisce a queste cose immediatamente (anche per attivare la PEC ci ho messo un bel po'), ma penso che questa iniziativa sia molto importante.

****

07- Nuovo Privacy shield, ossia "EU-US Data Privacy Framework"

Ci ricordiamo che il Privacy Shield, ossia l'accordo che regolava il traferimento dei dati da Europa a USA, fu invalidato a luglio 2020 (esattamente 3 anni fa). A luglio 2023, dopo esattamente 3 anni (meno qualche giorno) è stato approvato il "EU-US Data Privacy Framework (DPF)": https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721.

Grazie alla newsletter di Project:IN Avvocati, segnalo il sito web del DoC degli USA dove si possono trovare i requisiti per aderire al programma e dove sarà presente la lista dei partecipanti: https://www.dataprivacyframework.gov/.

Google è già nella lista (come ci fa sapere Not Boring Privacy): https://www.instagram.com/p/Cu1vPbCNAJs/.

Il nuovo accordo è stato oggetto di critica. Segnalo questo articolo dal titolo "Perché il nuovo data framework UE-USA avrà vita breve" per un breve commento: https://www.agendadigitale.eu/sicurezza/privacy/perche-il-nuovo-data-framework-ue-usa-avra-vita-breve/.

Io sarò cauto con i miei clienti, spingendoli a mantenere le modalità seguite da qualche anno, ossia dopo la Schrems II, ossia mantenere in Europa i sistemi informatici o, alla peggio, usare fornitori che adottano le SCC.

****

08- Garante privacy: illecite le email pubblicitarie senza consenso (anche se con il link per disiscriversi)

Il titolo è questo e spiega tutto: "Garante privacy: illecite le email pubblicitarie senza consenso Inserire un link per disiscriversi non rende l'invio lecito": https://www.gpdp.it/home/docweb/-/docweb-display/docweb/9903191#3.

Da ricordare questo link per poterlo mostrare ai tanti che parlano di "consenso soft".

****

09- Gli uomini possono fare tutto (Luglio 2023)

Seconda metà di giugno e prima metà di luglio piena di audit a cui avrei dovuto assistere per i clienti che ho assistito nella preparazione. Causa diversi cambi di pianificazione non l'ho potuto fare.

Nelle giornate che potevo, per contro, arrivavo sempre un po' più tardi e uscivo sempre un po' prima per portare ai o riprendere i bambini dai campi estivi. Una faticaccia. Ringrazio gli auditor che hanno evitato di fare domande troppo filosofiche in mia assenza e i clienti che mi hanno permesso di farlo.

****

EONL