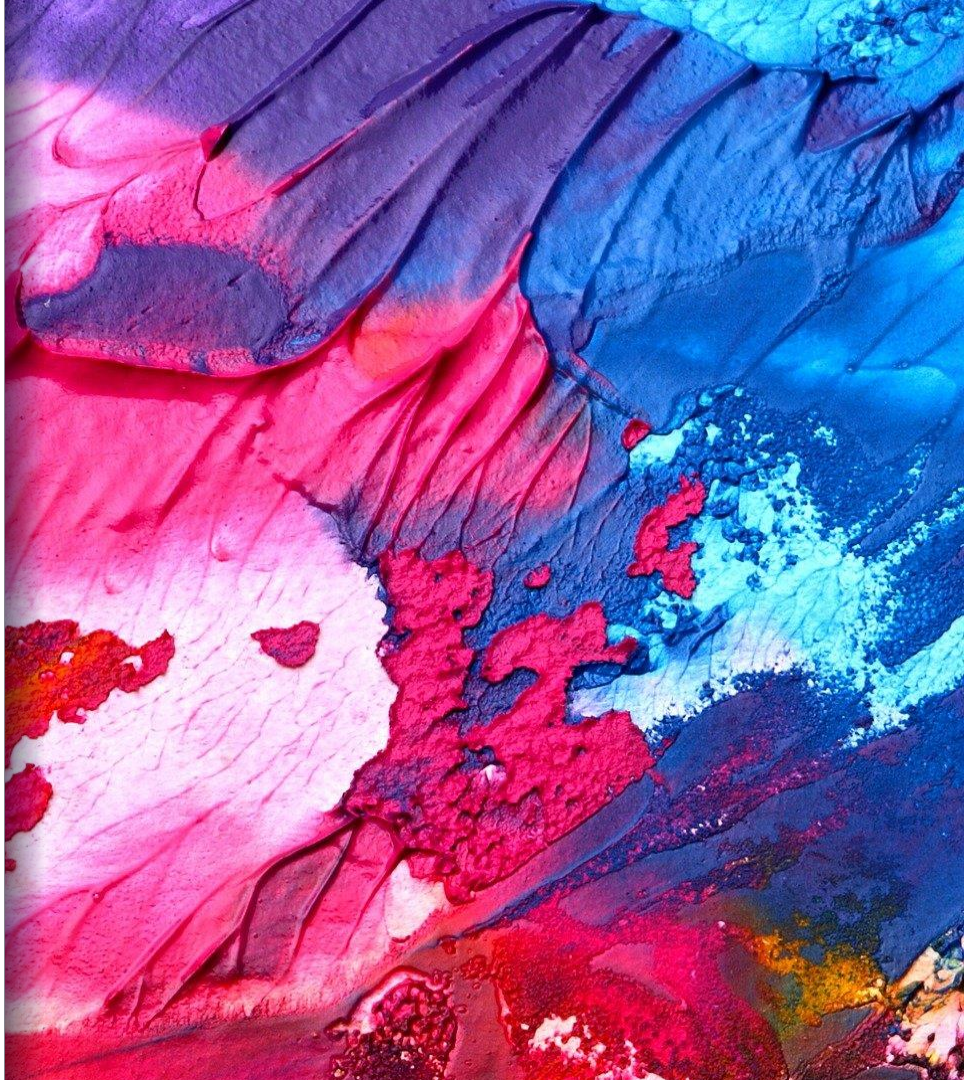
Fondazione Forense Bolognese

Progetto Atelier Privacy



Privacy Chat

Aggiornamenti & Privacy Pills

“Studio legale e attacchi informatici"

Protezione in pillole tra lavoro a distanza e conflitti internazionali

Avv. Lorenza Maria Villa

Webinar. 11 marzo 2022

CSIRT ITALIA - Computer Security Incident Response Team

Energenza Cyber Risk

Cybersecurity "standard"

quello che già ci dovrebbe essere ...

- Record dei dati trattati e dei responsabili esterni, dei contitolari e degli interessati
- Rilevazione dei trasferimenti di dati extra UE , verifica delle garanzie di trasferimento e censimento dei Data Importers con verifica delle garanzie offerte
- Inventario degli assets di trattamento: dispositivi utilizzati, software, applicazioni, servizi informatici utilizzati (es. servizi email, cloud storage)
- Misure di sicurezza tecniche
- Misure di sicurezza organizzative (es. access limitation policy, nomine / istruzioni e formazione del personale autorizzato al trattamento dei dati e all'utilizzo degli assets)
- Analisi del rischio
- Implementazione di misure di sicurezza a mitigazione, se necessario.
- Monitoraggio periodico

Misure di sicurezza "minime" e adeguate

- Password forti e autenticazione a 2 fattori (qualcosa che l'utente conosce, qualcosa che l'utente ha o qualcosa che l'utente è)
- Password uniche
- Aggiornamenti automatici
- Controllo dell'obsolescenza dell'hardware
- Sistemi di protezione perimetrale integrati (firewall, antivirus, sistemi di endpoint protection)
- Programmazione di back-up regolari automatici, back-up offline
- Limitazione e tracciabilità degli accessi
- Mezzi di comunicazione sicuri
- Limitazione delle app. sui dispositivi professionali
- Crittografia
- Safe browsing

Perchè io?

1.

Il problema non è "se", ma "quando"

2

Supply Chain attack

3

Phishing, Man-In-The-Middle attack, Spywares...

Supply Chain attack

Quando il malware ci viene trasmesso da un soggetto con il quale siamo in contatto o con il quale condividiamo strumenti informatici

Spillover

Siamo tutti direttamente collegati nel web.

L'attacco a un qualsiasi soggetto può generete un effetto a catena, passando da un collegamento a un altro

Cyber Pandemia

Fonti di rischio

- Piattaforme di comunicazione e interazione pubbliche e private
- Landing page corrotte, contenenti codici malevoli
- Attacchi di fishing, spear fishing, smishing e vishing
- Human factor

I nuovi virus

- Isaac Wiper - distribuito tramite eseguibili “.EXE” o librerie “.DLL”
- Le principali peculiarità consistono in:
  - ✓ enumerare le unità fisiche presenti sul sistema;
  - ✓ cancellare i primi 0x10000 byte di ciascun disco fisico rilevato, utilizzando il generatore pseudocasuale “ISAAC”;
  - ✓ enumerare le unità logiche e cancellare ricorsivamente i file in esse contenuti sovrascrivendoli con byte casuali tramite l’algoritmo “ISAAC PRNG”
- HermeticWizard - Worm distribuito tramite file “.DLL” “Wizard.dll”, il cui compito principale è distribuire HermeticWiper .
- HermeticRansom - Denominato anche “SonicVote”, Ransomware, Al termine del processo di crittografia viene rilasciata una nota di riscatto in cui si richiede alla vittima di contattare via mail gli attaccanti per ottenere le istruzioni per decriptare i file.

Fonte: CSIRT

Emergency Cybersecurity

quello che si deve implementare

- Minimizzazione della superficie d'attacco esterna
- Minimizzazione della superficie d'attacco interna
- Controllo degli accessi
- Monitoraggio
- Audit di sicurezza interno - Vulnerability assessment
- Pianificazione: Incident Response plan, Disaster Recovery Plan, Business continuity plan
- Zero - trust

Emergency Cybersecurity

quello che si deve implementare

(e Best Practices per il futuro)

Fonte: CSIRT

Misure organizzative/procedurali
Verifica della consistenza e disponibilità offline dei backup necessari al rispristino in particolare dei servizi di core business.
Identificazione dei flussi informativi e delle componenti direttamente interconnesse con partner e/o localizzate presso reti ucraine.
Identificazione degli asset critici per lo svolgimento delle principali attività (e.g. processi di business).
Applicazione del principio di privilegio minimo (least privilege) per i sistemi con relazioni di trust e/o con la possibilità di accesso da remoto.
Incremento delle attività di monitoraggio e logging.
Aggiornamento dei piani di gestione degli incidenti cyber in base alle eventuali modifiche architetturali introdotte.
Creazione, aggiornamento, mantenimento ed esercizio periodico di capacità di incident response, di un piano di continuità operativa e resilienza in caso di perdita di accesso o controllo di un ambiente informatico (IT) e/o operativo (OT).
Designazione di un team di risposta alle crisi con i principali punti di contatto, ruoli/responsabilità all'interno dell'organizzazione, inclusi tecnologia, comunicazioni, legal e continuità aziendale.
Assicurare la disponibilità del personale chiave, identificare i mezzi necessari a fornire un supporto immediato per la risposta agli incidenti.
Esercitare il personale nella risposta agli incidenti informatici assicurandosi che tutti i partecipanti comprendano i loro ruoli e compiti specifici.
Prestare particolare attenzione alla protezione degli ambienti cloud prima di trasferire file rilevanti per le attività della propria organizzazione. Inoltre, si raccomanda di utilizzare i controlli di sicurezza resi disponibili dalle piattaforme cloud.
Incrementare le attività di info-sharing con le strutture di sicurezza informatica con particolare riferimento allo CSIRT Italia.

Emergency Cybersecurity

quello che si deve implementare

(e Best Practices per il futuro)

Fonte: CSIRT

Misure tecniche
Prioritizzazione delle attività di patching dei sistemi internet-facing.
Verifica delle interconnessioni tra la rete IT e le reti OT prediligendo la massima segregazione possibile tra le stesse.
Monitoraggio degli account di servizio e degli account amministrativi per rilevare eventuali attività anomale.
Monitoraggio dei Domain Controller, in particolare gli eventi Kerberos TGS (ticket-granting service), al fine di rilevare eventuali attività anomalie.
Ricerca di processi e/o esecuzione di programmi da linea di comando che potrebbero indicare il dump di credenziali, in particolare monitorando i tentativi di accesso o di copia del file ntds.dit da un Domain Controller.
Monitoraggio dell'installazione di software di trasferimento file quali FileZilla e rclone, nonché dei processi associati agli strumenti di compressione o archiviazione.
Monitoraggio del traffico di rete analizzando picchi anomali nella connettività di rete in uscita, in particolare verso destinazioni inusuali quali provider VPS e VPN, nonché la rete TOR.
Prioritizzare le analisi a seguito di individuazione di codice malevolo (es. Cobalt Strike e webshell).
Assicurarsi che tutti gli accessi remoti richiedano l'autenticazione a più fattori (MFA), in particolare per servizi VPN, portali aziendali rivolti verso l'esterno (extranet) e accesso alla posta elettronica (es. Exchange Online).

Art. 32 GDPR

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso (art. 24)

a) la pseudonimizzazione e la cifratura dei dati personali (art. 4)

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento (art.

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Art. 32 GDPR

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati (Cons. 75)

3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri (art. 29)

Sanzioni in pratica

Violazione degli obblighi di sicurezza

Avvocati

Sanzioni in pratica

Violazione dei diritti degli interessati

Avvocati

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Provvedimento del 27 gennaio 2022 [9745860]

- **In data 25 marzo 2021 l'Avv. XX riceve un'istanza di esercizio dei diritti da parte di un interessato**
- **In data 05 maggio 2021 l'interessato comunicava all'Autorità Garante di non aver ricevuto alcun riscontro da parte dell'Avv. XX**
- **Il Garante invita l'Avv. XX ad aderire spontaneamente alla richiesta dell'interessato (11.06.2021)**
- **Con email in pari data, l'interessato comunica al Granite di aver ricevuto riscontro in data 20 maggio 2021**

Sanzioni in pratica

(aggiornamento)

Violazione dei diritti degli interessati da parte di un Avvocato

- **Sanzione comminata: ammonizione "per aver violato l'art. 12, par. 3 del GDPR**

3. Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 15 a 22 senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa.

Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste.

Il titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta.

Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.

Sanzioni in pratica

(aggiornamento)

Violazione dei diritti degli interessati da parte di un Avvocato

❑ Ritenuta infondatezza delle difese

A giustificazione della mancata predetta informazione all'interessato, l'Avv. XX ha rappresentato che "L'imprevisto superamento della scadenza ha comportato quindi che non rivolgessi istanza di proroga, concentrandomi comunque nel rispondere, come ritengo di aver fatto, nel più breve tempo possibile.".

Tuttavia, tale argomentazione non risulta idonea a giustificare la condotta del titolare che, avendo deciso di concentrarsi nel rispondere "nel più breve tempo possibile"- ma ben oltre i termini di legge - ha unilateralmente prorogato il termine di legge omettendo di adempiere all'obbligo di informativa del ritardo prescritto dalla disposizione eurounitaria, il cui adempimento era del resto di facile esecuzione, consistendo nella mera comunicazione all'interessato, senza particolari oneri o formalità, dei motivi del ritardo.

Risulta, pertanto, che l'Avv. XX, in qualità di titolare del trattamento, ha violato la disposizione di cui all'art. 12 paragrafo 3, del RGPD, non avendo comunicato all'interessato la proroga dei termini di legge per il riscontro alla richiesta di informazioni di quest'ultimo e dei motivi del ritardo, entro un mese dal ricevimento della richiesta.

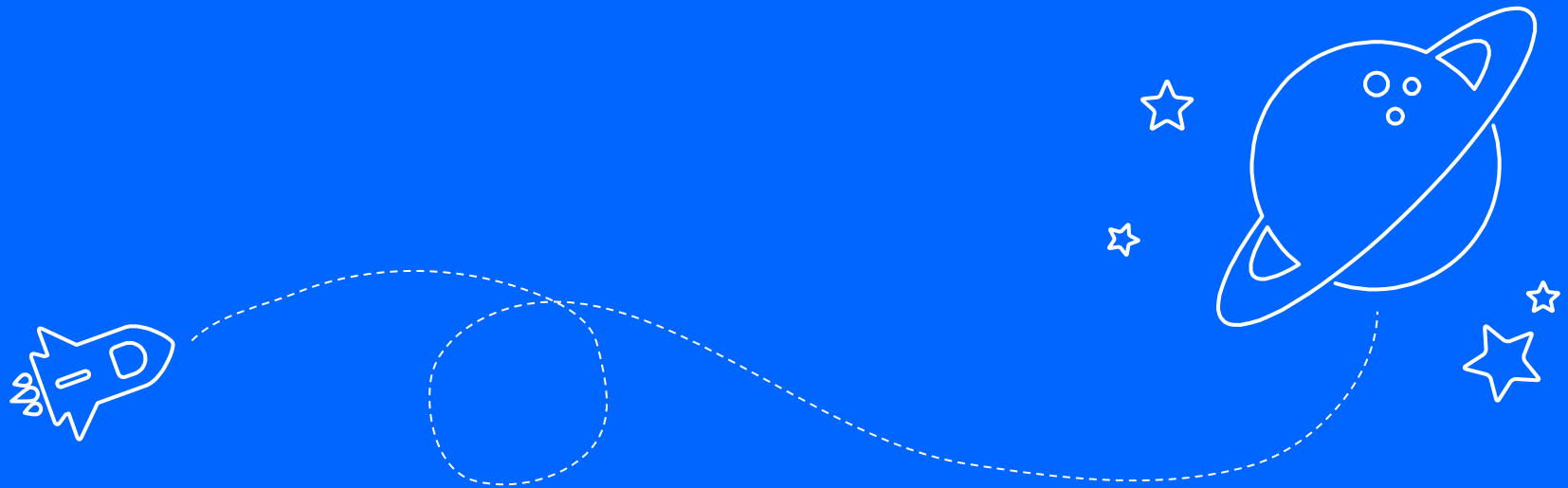
Sanzioni in pratica

(aggiornamento)

Violazione dei diritti degli interessati da parte di un Avvocato

- **Motivazione della sanzione comminata (ammonizione ed esclusione di sanzione pecuniaria)**

"... considerando che la condotta ha esaurito i suoi effetti, che il riscontro all'esercizio dei diritti dell'interessato è stato comunque spontaneamente fornito sia pur in ritardo, che non risultano eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento, che il livello del danno subito dall'interessato appare di lieve entità e che non sembrano sussistere eventuali fattori aggravanti, quali benefici finanziari conseguiti o perdite evitate, direttamente o indirettamente, quale conseguenza della violazione, si ritiene che nel caso di specie non ricorrano i presupposti per infliggere una sanzione amministrativa pecuniaria di cui all'art. 58, par. 2, lett. i) del Regolamento".



Grazie per l’attenzione

Appuntamento alla prossima *Privacy Chat*

Fondazione Forense Bolognese - Progetto Atelier Privacy


Fondazione Forense Bolognese
Atelier
Privacy