Chi sono

LLM in Intellectual Property

Master in Diritto Privato Europeo

Lead Auditor ISO 27001

Certified International Privacy Professional

Avv. Massimo Bacci

massimobacci@legalicappellinicarlesi.it

IPRights

PRIVACY DOODLES

DATA PROTECTION MADE SIMPLE

PRIVACY DOODLES®

DATA PROTECTION MADE SIMPLE

IPRights

Fornitori e NIS 2

Nuovi obblighi e opportunità nella Supply Chain

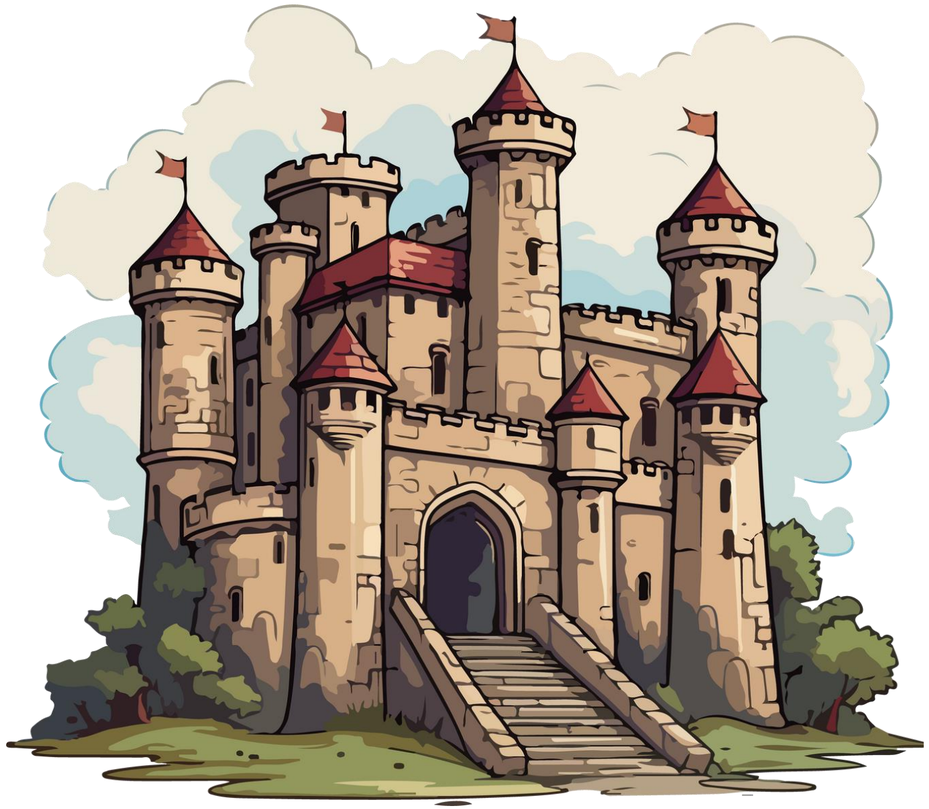
Avv. Massimo Bacci

Visit My Websites

privacydoodles.com

iprights.it

E se la nostra azienda fosse un castello da proteggere...



Mura e fossato = **Firewall**

Guardie = **Antivirus e sistemi di monitoraggio**

Trabocchetti = **Honey Pot**

... tutte queste misure di sicurezza sono inutili se abbassiamo il ponte levatoio.

Chi può abbassare il ponte levatoio?

- I dipendenti
- Alcuni fornitori

Il caso Solar Wind (2020)

🎯 Target

Software di gestione reti Orion di SolarWinds – usato da 18.000 clienti (aziende, enti pubblici, agenzie governative USA).

🛠 Metodo

Gli attaccanti compromettono la pipeline di build del software. Inseriscono codice malevolo (“Sunburst”) in un aggiornamento ufficiale.

📅 Cronologia

Marzo 2020: gli attaccanti inseriscono un codice malevolo (“Sunburst”) in un aggiornamento del software Orion.

Marzo–Giugno 2020: l’aggiornamento infetto viene distribuito a circa **18.000 clienti di SolarWind**, inclusi enti governativi statunitensi e grandi aziende private.

Dicembre 2020: la società di cybersecurity FireEye scopre l’intrusione dopo che i suoi stessi strumenti interni erano stati compromessi.

🎭 Attori

Gruppo APT29 / Cozy Bear (collegato ai servizi russi).

📌 Impatti

Accesso prolungato a reti sensibili.
Violazione di agenzie USA (es. Dipartimento del Tesoro, Commercio, Energia).
Allarme globale sulla cybersecurity della supply chain.

📚 Lezione appresa

Anche software “trusted” può diventare veicolo d’attacco. Serve monitoraggio continuo, controlli sulla filiera IT, Zero Trust.

Il caso Kaseya (2021)

🎯 Target

Software VSA di Kaseya – usato da Managed Service Provider (MSP) per gestire i sistemi dei clienti.

🛠 Metodo

Vulnerabilità zero-day in VSA on-premise.
Gli attaccanti sfruttano VSA per distribuire ransomware ai clienti MSP.
Catena: Kaseya → MSP → 1.500+ aziende colpite.

🎭 Attori

Gruppo REvil, collegato a criminali russi.

📅 Cronologia

2 luglio 2021: attacco lanciato durante il weekend del 4 luglio.

3 luglio 2021: Kaseya disconnette i server VSA.

11 luglio 2021: REvil scompare improvvisamente.

22 luglio 2021: Kaseya ottiene decryptor universal.

📌 Impatti

Imprese bloccate in tutto il mondo (es. catene di supermercati).
Ransomware diffuso da un fornitore “trusted”.
Richiesta di 70 milioni di dollari in Bitcoin.

📚 Lezione appresa

La supply chain IT è un moltiplicatore di rischio.

GDPR e NIS sulla Supply Chain

GDPR

Art. 28
Reg. UE 2016/679

Il titolare deve scegliere solo responsabili che offrano garanzie sufficienti in termini di misure tecniche e organizzative.

Necessità di un Data Processing Agreement.

Autorizzazione alla nomina di sub-responsabili (controllo della filiera).

Audit dei fornitori.

NIS 2

Art. 24
D.Lgs. 138/2024

Le misure sono basate su un approccio multi-rischio, volto a proteggere i sistemi informativi e di rete nonché il loro ambiente fisico da incidenti, e comprendono almeno i seguenti elementi:

d) sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardantii rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi.

Gestione del rischio cybersecurity nella catena di approvvigionamento

I processi di gestione del rischio di cybersecurity della catena di approvvigionamento sono identificati, stabiliti, gestiti, monitorati e migliorati dagli stakeholder dell'organizzazione.

I

GV.SC-01

Sono stabiliti e accettati dagli stakeholder dell'organizzazione un programma, una strategia, obiettivi, **politiche e processi di gestione del rischio** di cybersecurity della catena di approvvigionamento.

II

GV.SC-02

I **ruoli e le responsabilità in materia di cybersecurity** per fornitori, clienti e partner sono stabiliti, comunicati e coordinati internamente ed esternamente.

III

GV.SC-04

I fornitori sono noti e **prioritizzati in base alla criticità.**

IV

GV.SC-05

I **requisiti per affrontare i rischi di cybersecurity** nella catena di approvvigionamento sono stabiliti, prioritizzati e integrati **nei contratti** e in altri tipi di accordi con i fornitori e altre terze parti rilevanti.

V

GV.SC-07

I rischi posti da un fornitore, dai suoi prodotti e servizi e da altre terze parti sono compresi, registrati, prioritizzati, valutati, trattati e **monitorati nel corso della relazione**.

PRIVACY DOODLES®

DATA PROTECTION MADE SIMPLE

IPRights

Thank You

For Your Attention

Avv. Massimo Bacci

Visit My Websites

privacydoodles.com

iprights.it

Due parole su PRIVACY DOODLES

DATA PROTECTION MADE SIMPLE

Creazione e aggiornamento di un Sistema di Gestione Privacy
(Documenti redatti con tecniche di Legal Design)

Piattaforma in Cloud per gestire registri, documenti, inventari, analisi del rischio etc.

Formazione continua del personale

Consulenza All You Can Eat o servizi di DPO

www.privacydoodles.com