Come gestire la supply chain

Daniela Bruzzo
UO Sistemi Informativi - Regione Liguria

Perché la NIS2

- NIS1: Settori critici (energia, ICT, Sanità, Trasporti) sono interdipendenti tra loro.
- NIS2: Nuove minacce (pandemia, guerra ibrida).
- La protezione non solo dei sistemi ICT ma estesa a tutti gli oggetti connessi alla rete.
- Anche fornitori non IT possono bloccare IT: esempio fornitura di energia elettrica, gasolio per gruppi continuità.
- Ritrovata attenzione per le persone che se assenti dal lavoro potrebbe essere un problema di sicurezza.

Attacchi Cyber - Moldavia

CAUSA DEGLI ATTACCHI: MOTIVAZIONI POLITICHE

Interferenza ibrida: interruzione dei servizi, estorsione.

Danno reputazionale: attacchi mirati per ridurre la fiducia dei cittadini nelle istituzioni pubbliche.

Continua esplorazione e scansione delle infrastrutture critiche: sanità, energia, trasporti, servizi pubblici.

Inizio 2024: attacchi di phishing e malware a danno di dipendenti governativi.

Elezioni 2025: aumento esponenziale di disinformazione, phishing e intrusioni.

Attacchi Cyber – Ucraina

- Molto distruttivi:
  - ❖ Dicembre 2024 – registri statali del Ministero della Giustizia (nascite, decessi, matrimoni e proprietà immobiliari).
  - ❖ Marzo 2025: ferrovie ucraine (Ukrzaliznytsia).
- Coinvolgimento diretto della supply chain.
- Escalation degli attacchi cibernetici:
  - a) 2022 – 2.194;
  - b) 2023 – 2.541;
  - c) 2024 – 4.315;
  - d) da inizio 2025 - 3.600.

Ucraina – settore sanitario 2024

- Numero di attacchi phishing: oltre i 30
- Numero di attacchi alla rete: oltre i 30
- Continue scansioni del perimetro da parte dei Gruppi APT
- Continui attacchi alle web application
- Attacchi aumentati di 4 volte rispetto al 2023

Attacchi cyber all'ospedale pediatrico Okhmatdyt qualche giorno prima dei bombardamenti del 8 luglio 2024.

Gestione del rischio di cybersecurity della catena di approvvigionamento

- Massima attenzione alle forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete.
- Definizione di requisiti di sicurezza sulla fornitura coerenti con le misure di sicurezza definite.
- I rischi posti da un fornitore, dai suoi prodotti e servizi e da altre terze parti devono essere:

✓ compresi;
✓ registrati;
✓ prioritizzati;
✓ valutati;
✓ trattati;
✓ monitorati.

Cosa è richiesto ai soggetti NIS

- Inserimento di requisiti di sicurezza nelle richieste di offerta, bandi di gara, contratti, accordi e convenzioni.
- Valutazione dell'affidabilità dei fornitori:
  - eventuali vulnerabilità specifiche;
  - qualità complessiva dei loro prodotti;
  - pratiche di sicurezza informatica, con particolare riguardo a:
    - oggetto della fornitura;
    - capacità di garantire l'approvvigionamento; l'assistenza e la manutenzione nel tempo.
- Ruoli e responsabilità nell'ambito della fornitura.
- Livello di accesso del fornitore ai sistemi informativi e di rete.
- Accesso a proprietà intellettuale e ai dati anche sulla base della loro criticità.
- Impatto di una grave interruzione della fornitura.
- Tempi e costi di ripristino in caso di indisponibilità dei servizi.

Cambio di approccio per il fornitore

- Il rischio non è più "autonomo" ma diventa CONDIVISO tra tutti i soggetti della supply chain.
- Un «errore» dell'ultimo anello della catena si ripercuote su tutta la supply chain.

Occorre:

❖ Considerare la sicurezza informatica come fattore di competitività.

❖ Dimostrare un solido impegno verso la sicurezza informatica.

❖ Comprendere il proprio ruolo all'interno della supply chain.

L. 90/2024 Art. 14 – *Disciplina dei contratti pubblici di beni e servizi informatici*

Nei casi individuati ai sensi del comma 1, le stazioni appaltanti, comprese le centrali di committenza:

a) possono esercitare la facoltà di cui agli articoli 107, comma 2, e 108, comma 10, del codice dei contratti pubblici, di cui al decreto legislativo 31 marzo 2023, n. 36, se accertano che l'offerta non tiene in considerazione gli elementi essenziali di cybersicurezza individuati con il decreto di cui al comma 1;

b) tengono sempre in considerazione gli elementi essenziali di cybersicurezza di cui al comma 1 nella valutazione dell'elemento qualitativo, ai fini dell'individuazione del miglior rapporto qualità/prezzo per l'aggiudicazione;

c) nel caso in cui sia utilizzato il criterio del minor prezzo, ai sensi dell'articolo 108, comma 3, del codice di cui al decreto legislativo n. 36 del 2023, inseriscono gli elementi di cybersicurezza di cui al comma 1 del presente articolo tra i requisiti minimi dell'offerta.

Grazie

novembre, 2025