Clusit
Associazione Italiana per la Sicurezza Informatica

ASTREA Advanced Security, Training Research, Events Agency

SECURITY SUMMIT

Security Summit

Milano 19-20-21 marzo 2024

IN-House: I rischi «Privacy» e «Cyber» nelle forniture delle pubbliche amministrazioni

Il governo della supply Chain nella gestione degli Incidenti cyber

Pier Paolo Gruero, CISO, CSI Piemonte

20 marzo 2024

Pier Paolo Gruero

RESPONSABILE FUNZIONE RETE, CYBERSECURITY E IDENTITÀ DIGITALE

CHIEF INFORMATION SECURITY OFFICER

CSI your digital partner

Piano Triennale AgID

Strategia e principi guida:

- fornire strumenti alla Pubblica Amministrazione per erogare servizi esclusivamente in modalità digitale, rendendo più efficaci e veloci i processi di interazione con cittadini, imprese e altre pubbliche amministrazioni.

- favorire lo sviluppo di una società digitale, dove i servizi mettono al centro i cittadini e le imprese, attraverso la digitalizzazione della Pubblica Amministrazione che costituisce il motore di sviluppo per tutto il Paese

Transizione Digitale

opportunità senza precedenti

sfide significative in termini di cyber security

Contesto

Secondo **il rapporto dell'ENISA "Good Practices for supply chain cybersecurity", pubblicato lo scorso giugno 2023**, si evidenzia che un'ampia percentuale delle organizzazioni intervistate, compresa tra il 39% e il 62%, ha subito un incidente informatico causato da terze parti

nel 66% dei casi di attacchi alla supply chain analizzati, **i fornitori non erano consapevoli di come fossero stati compromessi** o **mancavano di trasparenza al riguardo**

Contesto - NIS2 e DDL Cybersicurezza

La direttiva **NIS2 richiede che i soggetti in perimetro affrontino i rischi di cyber security nelle catene di approvvigionamento e nelle relazioni con i fornitori**.

L'articolo 21, in particolare, richiede che tali enti **adottino misure appropriate e proporzionate di gestione del rischio di cyber security** a livello sia tecnico sia operativo sia organizzativo

DDL Cybersicurezza (allo studio del Parlamento) prevede **l'obbligo di segnalazione degli incidenti ad ACN entro 24 ore** e quello di **notifica entro 72 ore** !!

Gestione degli Incidenti e Supply Chain

- Le pratiche per la cybersecurity siano stabilite, seguite, mantenute e documentate **ma soprattutto condivise**
- Il personale responsabile delle attività di cybersecurity della supply chain ICT/OT **possegga le competenze e le conoscenze necessarie per svolgere i ruoli e responsabilità assegnati**
- Le **responsabilità e l'autorità** per lo svolgimento delle attività di cybersecurity della supply chain ICT/OT **siano definite ed assegnate al personale**
- **Importanti dipendenze** dai fornitori IT e OT (ovvero soggetti esterni da cui dipende l'erogazione della funzione, inclusi i partner operativi) **devono essere identificate**

Gestione degli Incidenti e Supply Chain

- Devono essere **noti a priori i punti di contatto** (CISO, DPO, SOC, etc..) di tutti i soggetti al fine di ridurre i tempi operativi -> **gestione del rapporto «preventiva»**
- Coinvolgere la Supply Chain in esercitazioni «table top» di **simulazioni incidenti** al fine di testare procedure e tempi di reazione
- Istituzione di un **tavolo di crisi congiunto** durante un indicente al fine di coordinare anche il corretto livello di comunicazione
- **monitorare i cambiamenti nel profilo di rischio di un fornitore,** poiché il panorama delle minacce e la superficie di attacco sono in continua evoluzione e cambiamento

Q&A

CONTATTI:

PIERPAOLO.GRUERO@CSI.IT