Choose Scandinavian trust

Certificazione Cyber Security per prodotti IoT

Oscar Frau

15/07/2021

Cybersecurity

Salvaguardia di sistemi, dispositivi informatici e dati sensibili.

Possibili applicazioni IoT:

Giocattoli per bambini e baby monitor
Sistemi di sicurezza per domotica
Elettrodomestici
Telecamere intelligenti
Smart TV

Nemko

Dati sensibili

Dati ed informazioni scambiate tra dispositivi:

Personale

Finanziario

Social Network

Aziendali

Governative

Rischi

Cosa comporta la perdita di riservatezza?

Danno economico

Perdita della reputazione

Minacce

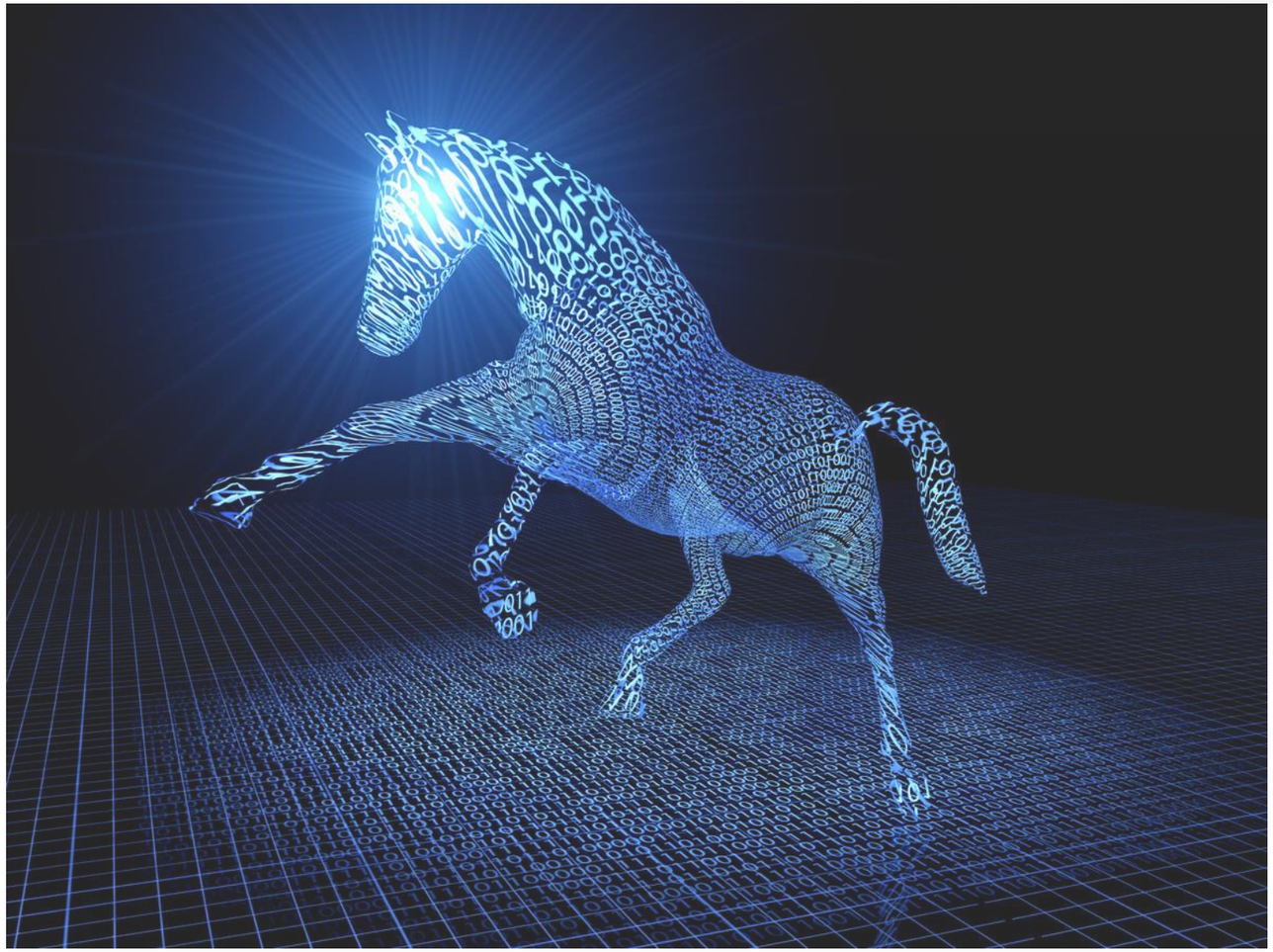
ATTACCHI INFORMATICI

Malware (Worm, Virus), Trojan, Ransomware, DDoS, …

Livello Amatoriale, Hacker

Provenienza Interna, Esterna

Vulnerabilità hardware, software



Minacce

PIU' DIFFUSE TIPOLOGIE DI ATTACCHI INFORMATICI

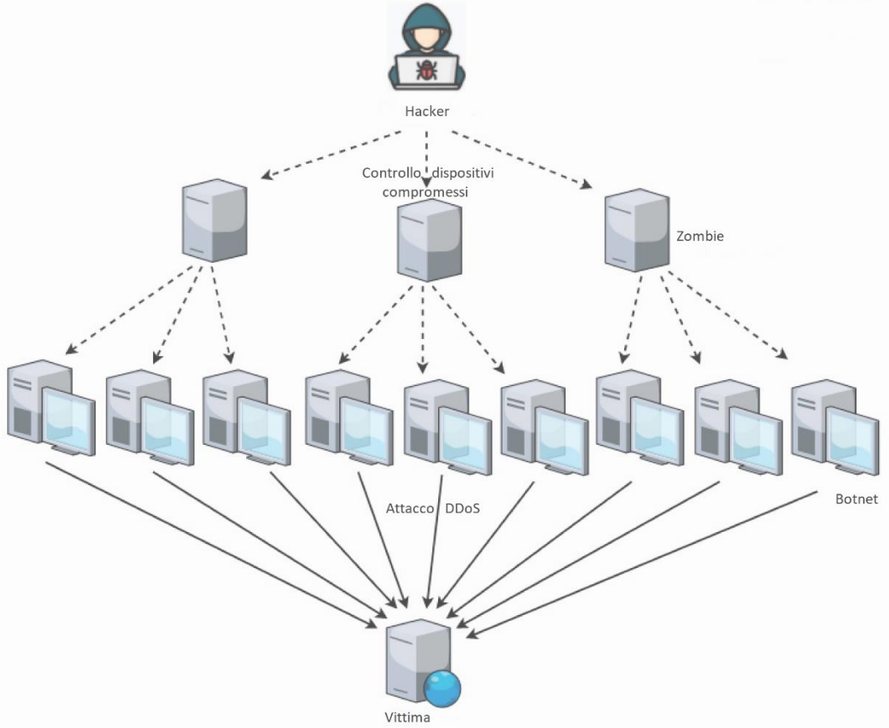
VIRUS (richiede l'interazione dell'utente)

WORM (autoreplicante, sfrutta la rete per propagarsi e non richiede l'interazione dell'utente)

TROJAN (mascherato da sw innocuo, nasconde codice malevolo)

DDoS (blocco di sistemi o dispositivi tramite sovraccarico)

RANSONWARE (richiesta di riscatto per sbloccare sistemi, dispositivi o file infetti)



Nemko

Minacce

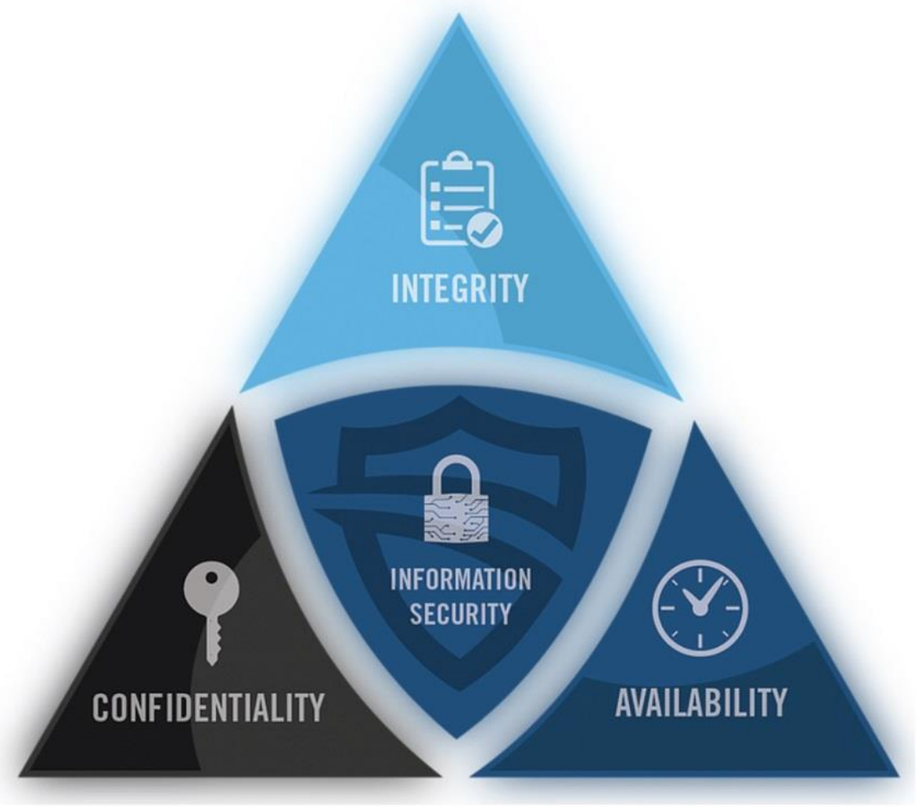
MAGGIORI VETTORI DI ATTACCHI INFORMTICI

CIA

Confidenzialità:
dati a disposizione dei soli soggetti autorizzati
(→ criptografia dei dati, user ID/psw, doppia autenticazione)

Integrità:
dati non alterabili da soggetti non autorizzati (→ controllo degli accessi, checksum)

Disponibilità:
dati sempre consultabili (→ backup)



Nemko

Standard e Regolamenti

Cyber Security Act
Regulation 2019/881

Common Criteria ISO/IEC 15408

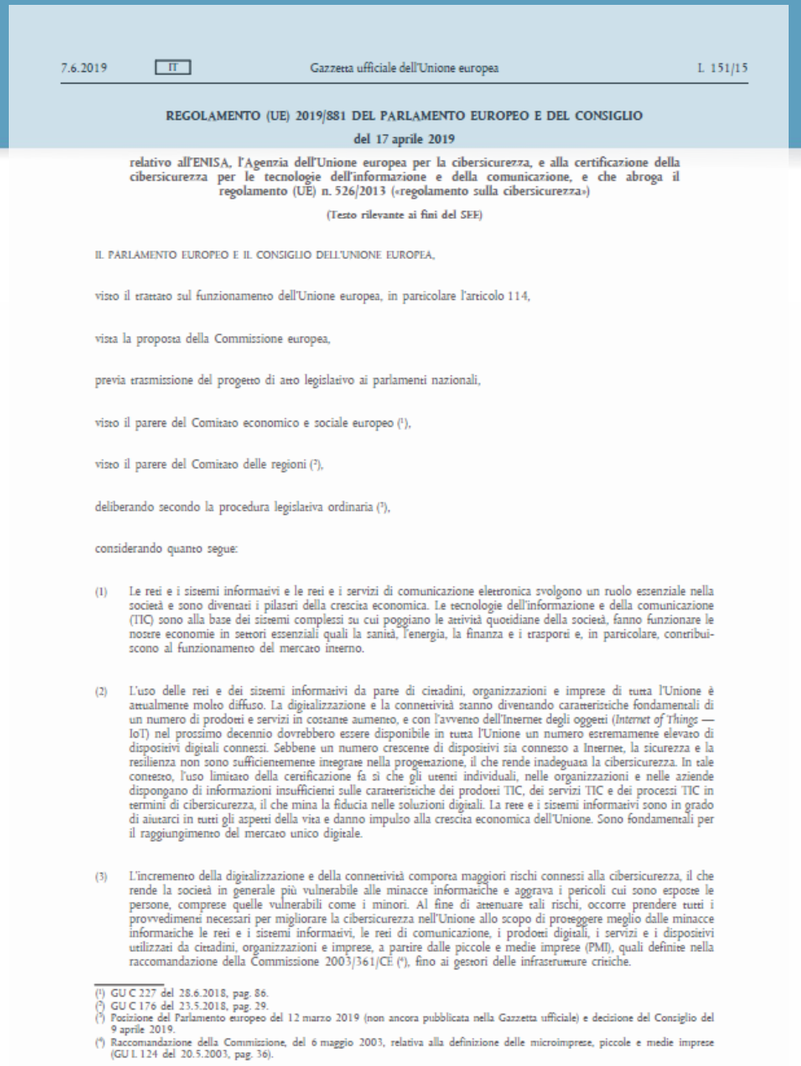
ETSI EN 303 645 V2.1.1 (2020-06)

CSA Regulation 2019/881

Raggiungimento e mantenimento un livello elevato in materia di sicurezza informatica.

Obiettivi e compiti dell’ENISA

Definizione di un quadro per l’istituzione di sistemi europei di certificazione



7.6.2019 IT Gazzetta ufficiale dell'Unione europea L 151/15

REGOLAMENTO (UE) 2019/881 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
del 17 aprile 2019

relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»)

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo (1),

visto il parere del Comitato delle regioni (2),

deliberando secondo la procedura legislativa ordinaria (3),

considerando quanto segue:

(1) Le reti e i sistemi informativi e le reti e i servizi di comunicazione elettronica svolgono un ruolo essenziale nella società e sono diventati i pilastri della crescita economica. Le tecnologie dell'informazione e della comunicazione (TIC) sono alla base dei sistemi complessi su cui poggiano le attività quotidiane della società, fanno funzionare le nostre economie in settori essenziali quali la sanità, l'energia, la finanza e i trasporti e, in particolare, contribuiscono al funzionamento del mercato interno.

(2) L'uso delle reti e dei sistemi informativi da parte di cittadini, organizzazioni e imprese di tutta l'Unione è attualmente molto diffuso. La digitalizzazione e la connettività stanno diventando caratteristiche fondamentali di un numero di prodotti e servizi in costante aumento, e con l'avvento dell'Internet degli oggetti (*Internet of Things* — IoT) nel prossimo decennio dovrebbero essere disponibile in tutta l'Unione un numero estremamente elevato di dispositivi digitali connessi. Sebbene un numero crescente di dispositivi sia connesso a Internet, la sicurezza e la resilienza non sono sufficientemente integrate nella progettazione, il che rende inadeguata la cibersicurezza. In tale contesto, l'uso limitato della certificazione fa sì che gli utenti individuali, nelle organizzazioni e nelle aziende dispongano di informazioni insufficienti sulle caratteristiche dei prodotti TIC, dei servizi TIC e dei processi TIC in termini di cibersicurezza, il che mina la fiducia nelle soluzioni digitali. La rete e i sistemi informativi sono in grado di aiutarci in tutti gli aspetti della vita e danno impulso alla crescita economica dell'Unione. Sono fondamentali per il raggiungimento del mercato unico digitale.

(3) L'incremento della digitalizzazione e della connettività comporta maggiori rischi connessi alla cibersicurezza, il che rende la società in generale più vulnerabile alle minacce informatiche e aggrava i pericoli cui sono esposte le persone, comprese quelle vulnerabili come i minori. Al fine di attenuare tali rischi, occorre prendere tutti i provvedimenti necessari per migliorare la cibersicurezza nell'Unione allo scopo di proteggere meglio dalle minacce informatiche le reti e i sistemi informativi, le reti di comunicazione, i prodotti digitali, i servizi e i dispositivi utilizzati da cittadini, organizzazioni e imprese, a partire dalle piccole e medie imprese (PMI), quali definite nella raccomandazione della Commissione 2003/361/CE (4), fino ai gestori delle infrastrutture critiche.

(1) GU C 227 del 28.6.2018, pag. 86.
(2) GU C 176 del 23.5.2018, pag. 29.
(3) Posizione del Parlamento europeo del 12 marzo 2019 (non ancora pubblicata nella Gazzetta ufficiale) e decisione del Consiglio del 9 aprile 2019.
(4) Raccomandazione della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese (GU L 124 del 20.5.2003, pag. 36).

Nemko

CSA Regulation 2019/881

Art.8

definisce i compiti dell'ENISA (European Union Agency for Cybersecurity)
supporta e promuove lo sviluppo e l'implementazione delle politiche dell'Unione Europea sulla certificazione monitorando sviluppi ed evoluzioni di standard specifici e raccomandando l'utilizzo di schemi di certificazione preparati in base alle linee guida definite all'art.54

Nemko

CSA Regulation 2019/881

Art.51

OBIETTIVI degli SCHEMI di CERTIFICAZIONE

Protezione e disponibilità dei dati
Identificazione delle vulnerabilità
Registrazione degli eventi
Ripristino dei dati
Definizione del livello di sicurezza minimo

CSA Regulation 2019/881

Art.52

LIVELLI di GARANZIA degli SCHEMI di CERTIFICAZIONE

Tre livelli di certificazione

(liv. base può essere volontario)

La valutazione va eseguita in funzione del rischio associato all'uso previsto e in termini di probabilità e impatto dell'attacco.

Nemko

CSA Regulation 2019/881

Art.52

LIVELLI di GARANZIA degli SCHEMI di CERTIFICAZIONE

LIVELLO BASE

valutazione rivolta ad accertare e ridurre al minimo i rischi derivanti da possibili attacchi eseguiti da amatori o hacker di basso livello.

La valutazione prevede l'esame della documentazione prodotta a supporto dell'oggetto da esaminare.

Nemko

CSA Regulation 2019/881

Art.52

LIVELLI di GARANZIA degli SCHEMI di CERTIFICAZIONE

LIVELLO INTERMEDIO

valutazione rivolta ad accertare e ridurre al minimo i rischi derivanti da possibili attacchi eseguiti da hacker con competenze e strumenti di medio livello, rispetto alle vulnerabilità note.

La valutazione prevede:

. Esame della documentazione;

. Corretta individuazione delle vulnerabilità;

. Test delle contromisure.

Nemko

CSA Regulation 2019/881

Art.52

LIVELLI di GARANZIA degli SCHEMI di CERTIFICAZIONE

LIVELLO ELEVATO

valutazione rivolta ad accertare e ridurre al minimo i rischi derivanti da possibili attacchi eseguiti da hacker con competenze e strumenti di livello avanzato.

La valutazione prevede:

. Esame della documentazione;

. Test delle contromisure;

. Corretta individuazione delle vulnerabilità;

. Test di resilienza.

Nemko

CSA Regulation 2019/881

Art.54

ELEMENTI dello SCHEMA di CERTIFICAZIONE

Oggetto e scopo
Standard adottati
Livello di sicurezza
Requisiti degli organismi di valutazione
Regole per il mantenimento della conformità nel tempo
Contenuto e periodo di validità del certificato

Common Criteria ISO/IEC 15408

CONCETTI BASE

Richiama i princìpi CIA

Princìpi generali di valutazione

- Security Functional Requirements
- Security Assurance Requirements

Security Target

Protection Profiles


INTERNATIONAL STANDARD

ISO/IEC 15408-1

Second edition
2005-10-01

Information technology — Security techniques — Evaluation criteria for IT security —

Part 1:
Introduction and general model

Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI —

Partie 1: Introduction et modèle général

Reference number
ISO/IEC 15408-1:2005(E)

© ISO/IEC 2005

Common Criteria ISO/IEC 15408

OBIETTIVI di SICUREZZA
(sicuro per far cosa?)

contrastare le minacce in relazione alle funzionalità del prodotto (funzionalità di sicurezza).

AMBIENTE di SICUREZZA
(sicuro in quale contesto?)

definizione dell'ambiente di utilizzo del prodotto e delle relative minacce da contrastare.

Nemko

Common Criteria ISO/IEC 15408

REQUISITI di GARANZIA
(sicuro a fronte di quali verifiche?)

Security Target / Protection Profiles

Nemko

Common Criteria ISO/IEC 15408

SECURITY TARGET

Caratteristiche dettagliate del prodotto

- ToE (Target of Evaluation)
- Soggetti (risorse attive)
- Oggetti (risorse passive)
- Interazione dell'utente con il ToE

Identificazione delle vulnerabilità

Contromisure da adottare → requisiti funzionali

Livello di sicurezza → requisiti di garanzia

Nemko

Common Criteria ISO/IEC 15408

PROTECTION PROFILES

Ha le stesse finalità del ST

Contiene le stesse informazioni del ST

ST → l'oggetto della valutazione è il prodotto specifico

PP → l'oggetto della valutazione è la classe di prodotto

Nemko

Common Criteria ISO/IEC 15408

VANTAGGI dei CC

Competenza tecnica nella valutazione

Approfondimento delle contromisure

Maggiori livelli di garanzia disponibili

Standardizzazione dei requisiti per tipologia di prodotto (PP)

Nemko

Common Criteria ISO/IEC 15408

SVANTAGGI dei CC

Tempistiche della valutazione

Costi

Perdita della certificazione se vengono meno le condizioni di utilizzo

ETSI EN 303 645 V2.1.1 (2020-06)

Riunisce le pratiche più comuni in materia di sicurezza informatica

E’ focalizzata sui risultati delle disposizioni

Consente di adattare le disposizioni al prodotto

ETSI EN 303 645 V2.1.1 (2020-06)

OBIETTIVI

Identificare i requisiti di sicurezza di base

Convalidare tali requisiti

Mantenere il livello di sicurezza nel tempo

Nemko

ETSI EN 303 645 V2.1.1 (2020-06)

REQUISITI di CONFORMITÀ
(Annex B – tabella b.1)

Gestione del profilo utente

Gestione del software

Gestione delle vulnerabilità

Resilienza

Nemko

Servizi Nemko

COMMON CRITERIA

Laboratorio Nemko accreditato fino a EAL5

Supporto nel processo di certificazione e nella stesura della documentazione

Servizi Nemko

ETSI EN 303 645 V2.1.1 (2020-06)

Schema di certificazione Nemko

Nemko Cyber Secure Product Certification

Valutazione eseguita in accordo ad uno standard europeo

Valutazione eseguita da un organismo accreditato

Servizi Nemko

ATTESTATO → Valutazione + attestato di conformità

CERTIFICAZIONE → Attestato + schema per l'autovalutazione in caso di modifiche (richiederà audit di qualità)

Questions

Nemko

Choose Scandinavian trust

Thank you