

Sicurezza fisica



Massimo Carnevali

Il materiale di questo corso è distribuito con licenza Creative Commons 4.0 Internazionale: Attribuzione-Condividi allo stesso modo.

<https://creativecommons.org/licenses/by-sa/4.0/>

Dove note sono state citate le fonti delle immagini utilizzate, per le immagini di cui non si è riusciti a risalire alla fonte sono a disposizione per ogni segnalazione e regolarizzazione del caso.

Massimo Carnevali

posta@massimocarnevali.com

<https://it.linkedin.com/in/massimocarnevali>

"Master lock with root password" di Scott Schiller - Flickr: Master lock, "r00t" password. Con licenza CC BY 2.0 tramite Wikimedia Commons

Sicurezza fisica

- Sicurezza fisica
- Sicurezza hardware

..

Sicurezza fisica

La maggior parte delle protezioni logiche falliscono (o comunque si indeboliscono) se si riesce ad avere l'accesso fisico ai dispositivi. Per garantire la disponibilità del dato debbo ovviamente anche proteggere il device fisico che lo contiene o lo trasporta.

Armadi (rack) e sale con sistemi di controllo accessi (chiavi, badge, sistemi biometrici) organizzati su più livelli

Accesso fisico ai locali aziendali solo alle persone autorizzate (badge in vista, trashing!)

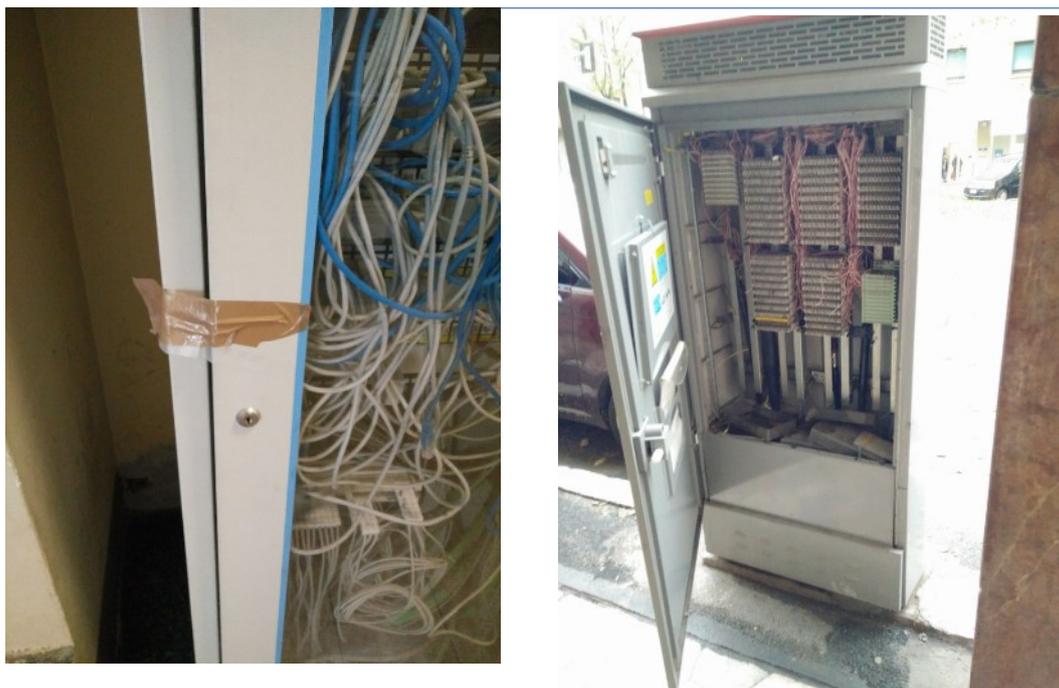
Protezioni contro il fuoco, il calore, l'acqua

Protezione da alterazioni della corrente elettrica

Ventilazione e condizionamento HVAC (

<https://en.wikipedia.org/wiki/HVAC> Heating, ventilation, air conditioning)

Sicurezza fisica



Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo

4

Questo ad esempio non si fa (zona aperta al pubblico e di passaggio e armadio di strada con fibre e linee telefoniche)

Endpoint protection

- Application Control (HIPS)
- Gestione del personal firewall
- Gestione e blocco dei dispositivi periferici
- Controllo delle connessioni di rete
- Controllo dei file
- Verifica degli usi propri dei dati e della postazione
- Blocco esecuzione applicazioni (whitelist)

Endpoint protection

Sono sistemi integrati che forniscono agli amministratori dei client un controllo esteso e centralizzato sui dispositivi, in termini di:

Application Control (HIPS)

Gestione del personal firewall

Gestione e blocco dei dispositivi periferici (USB)

Controllo delle connessioni di rete

Controllo dei file

Verifica degli usi propri dei dati e della postazione

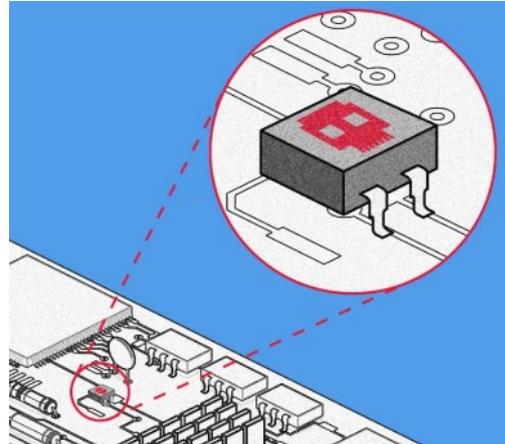
Blocco esecuzione applicazioni (whitelist)

Necessitano spesso di una fase di apprendimento.

Complessi da installare e da gestire. Possono interferire con l'utente finale.

Sicurezza hardware

Supply chain security



Planting Tiny Spy Chips in Hardware Can Cost as Little as \$200

A new proof-of-concept hardware implant shows how easy it may be to hide malicious chips inside IT equipment.

Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo

6

Da chi ho comperato il mio HW?
Sempre più facile intervenire su hw prima che
arrivi all'acquirente, se sono
stato/governo/grosso ente/azienda di valore
debbo pormi il problema dei miei fornitori.
Esempi 5G/Huawey, CISCO ecc.

<https://www.wired.com/story/plant-spy-chips-hardware-supermicro-cheap-proof-of-concept/>

Sicurezza hardware

Supply chain security

The SolarWinds Cyber-Attack: What You Need to Know

Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo

7

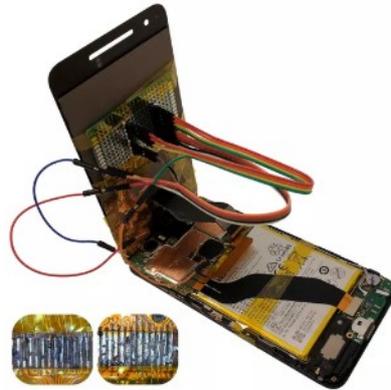
Vale anche per la catena di acquisto del software.

Solarwinds software di gestione delle reti attaccato a monte colpisci tutti gli acquirenti. NotPetya è nato anche lui così.

<https://www.cisecurity.org/solarwinds/>

Sicurezza hardware

Manutenzione e riparazioni



Hacked replacement touchscreens could hijack your smartphone

Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo

8

Se qualcuno mette mano fisicamente al mio dispositivo faccio fatica a difendermi.
Attenzione anche a chi mi ripara il telefono

<https://www.theverge.com/2017/8/21/16177916/malicious-replacement-touch-screens-control-smart-phone>