Quando si sottovaluta il Network nell' IoT

Premesse:

Abbiamo un network, sia per office sia per automazione, di circa 100 switch con mediamente 3.000 device di vario genere collegati quotidianamente

Il network è segmentato in 59 VLAN; alcune di queste protette da firewall fisico, altre da ACL

Il network automazione è molto allo stato primordiale; ancora comanda la scuola della "chiavetta" per configurare i PLC.

Lato automazione abbiamo un sistema di controllo degli avvitatori che segnalano al sistema se e come è stato avvitato un determinato bullone.

In caso di mancanza del sign il sistema blocca la catena di montaggio automaticamente.

I sign vengono raccolti su macchine virtuali e su SAP

Problematica riscontrata.

Una mattina, randomicamente, gli utenti venivano buttati fuori da SAP, altri proprio non entravano. Stesso comportamento l'avevano anche i thin client (circa 500).

In prima battuta abbiamo pensato a un problema di SAP ma dopo alcune ore di controlli non appariva nulla e quindi scartato.

Il network non presentava nessun tipo di problematiche. Gli switch installati, Juniper, permettono di effettuare delle configurazioni "prive" di stp pertanto il network risulta molto più stabile e sicuro.

Dopo diverse ore ho riscontrato un numero anomalo di MAC address su una porta di uno switch periferico. Controllando fisicamente cosa vi era collegato è saltato fuori che era un IP TV con OS Android.

Scollegando tutto è ripartito.

Cosa è successo:

Il televisore, avendo un OS, è di fatto un PC ed era stato collegato dal personale non IT senza configurarlo. Di default aveva abilitato il DHCP server.

Sede Legale/Operativa: Cso Lodi 101 – 20139 Milano – C.F./P.IVA 04289730964 - Tel. 02 91945363 – Fax 02 55017955 - Cell. 348 0175837
Uffici Collegati: Milano, Roma, Genova, Palermo
www.f10consulting.net - **support@f10consulting.net**
force10consultingsrl@pec.f10consulting.net

Questo cosa ha provocato:
Utenti che non si collegavamo perchè su network differenti
La sincronizzazione dei 2 server DHCP "ufficiali" si è interrotta con la conseguenza che entrambi i server si sono eletti master rilasciando gli stessi IP Address.
I PC fisici si buttavano fuori perchè scoprivano il duplicato ma i thin client no. Logicamente sono collegati direttamente al SAP
Con la conseguenza che si presentavano query SAP da stessi IP Address ma MAC differenti.
Risultato server SAP bloccato e quindi produzione bloccata
Come avremmo potuto prevedere.
Sugli switch Juniper (ma anche su molti switch di altri vendor di fascia alta) è possibile attivare:

- controlli su da chi un client può ricevere le risposte DHCP
- controlli di spoofing; nessuno può ricevere pacchetti per me mettendosi il mio mac address.
- controlli sul numero di MAC address presenti su una porta (un PC ha un MAC Address; se ne ho di più perchè?)
- controlli su quante volte posso cambiare il MAC address su una porta (perchè un PC si cambia il MAC address?)

Questi semplici controlli avrebbero bloccato l'attacco al sorgere del problema. Un buon sistema di monitoraggio ci avrebbe avvertito dello scampato pericolo.
Un buon firewall ci avrebbe diviso i network
Peccato che il cliente non aveva ancora voluto implementarli perchè ritenuti "limitativi"

Tutta la produzione del turno di notte e quella della mattina successiva è stata bloccata. Quanto è costato quel televisore IP ?
Qualche giorno dopo abbiamo implementato i controlli, riattaccato il televisore (senza aver fatto nessuna modifica di configurazione) e ... i blocchi sono immediatamente intervenuti e non abbiamo provocato nessun disservizio.
Considerazione:
oramai gli attacchi, fraudolenti o no, stanno arrivando da device privi di controllo.
Se un cripto locker è possibile bloccarlo attraverso l'esplosione degli allegati in server in cloud sacrificabili, i virus portati internamente da i device mobili è molto più complesso.
Sta al progettista del network e della sicurezza prevederli e mettere il sistema al sicuro.
Il vantaggio dell' IoT è indiscutibile anche a fronte di una sottovalutazione di potenziale problema come quello descritto.

Basta configurare il network e non accederlo in modalità di default.

Sede Legale/Operativa: Cso Lodi 101 – 20139 Milano – C.F./P.IVA 04289730964 - Tel. 02 91945363 – Fax 02 55017955 - Cell. 348 0175837
Uffici Collegati: Milano, Roma, Genova, Palermo
www.f10consulting.net - **support@f10consulting.net**
force10consultingsrl@pec.f10consulting.net