nethesis

Best Practice: Hardening Security

Davide Marini

Finalità del Webinar

- Condividere best practice di configurazione
- Ricevere feedback e discutere eventuali ulteriori best practice

È un webinar sul GDPR?

No, anzi Sì

Con la nuova normativa:

Sarà obbligatorio notificare all'Autorità, entro 72 ore dall'avvenimento, qualsiasi violazioni di dati e informare del problema le persone a cui si riferiscono i dati

Bisognerà dimostrare di aver messo in atto tutti i mezzi possibili per proteggere la propria infrastruttura e per evitare possibili attacchi, pena sanzioni fino a 20 milioni di euro o pari al 4% del fatturato internazionale.

- Responsabilizzazione e misure adeguate
  - Valutazione del rischio (es: firewall in strutture sanitarie)
  - Azioni commisurate al contesto

È un webinar sul GDPR?

Nomine di figure di responsabilità e gestione dati (es: Responsabile protezione dei dati/DPO)

Gestione **progettuale** della sicurezza che coinvolge l'intera infrastruttura IT

Il singolo prodotto può avere tecnologie adeguate ma non assicura la compliance dell'infrastruttura

Non esiste la sicurezza assoluta

- La quantità di sicurezza ottenibile dipende da ciò a cui possiamo rinunciare pur di ottenerla

- Richiede sempre un compromesso tra rinuncia e sicurezza

- La valutazione del compromesso deve tenere conto di:
  - Pericoli (in quali modi si può nuocere al sistema)
  - Rischi (probabilità di un evento pericoloso e gravità delle conseguenze)

La sicurezza è un processo

- Sistema complesso, comprende tutti gli elementi coordinati al conseguimento di un effetto
  - Coinvolge tutto l'ecosistema

La sicurezza è un processo

- Non esiste un solo prodotto(strumento) in grado di proteggere da tutte le minacce
- Insieme di procedure, pratiche e tecnologie

- Infrastruttura e topologia di rete
- Dispositivi collegati (PC, server, altri device)
- Firewall

È sufficiente un dispositivo compromesso (*anello debole*) per mettere a rischio l'integrità della rete

Minacce comuni

- Ransomware
- Phishing
- Attacchi informatici veri e propri (invio spam->blacklist)

Obbiettivi

- Evitare infezione delle macchine
- Contenere i danni in caso di infezione

Proteggere macchine della rete

Tutte le macchine della rete devono utilizzare:

- Sistemi operativi attuali supportati dal produttore e costantemente aggiornati

- Sistemi di protezione (antivirus etc.)
  - Es: Scansione chiavette USB

Proteggere macchine della rete

Se su alcune macchine non è possibile assicurare queste caratteristiche:

- Confinare macchine su reti dedicate in modo da limitare i danni

  Es:
  Rete Laboratorio per i pc dei clienti (Blue)

Proteggere macchine della rete

Mai introdurre nella LAN macchine esterne

- Reti dedicate per accessi Wireless
- Rete hotspot per ospiti
  - Abilitare client isolation

Dispositivi particolari (es: telecamere IP)

Tipicamente non assicurano robustezza e aggiornamenti continui

- Meglio confinarli su una rete Blue/Orange

Proteggere macchine della rete

Password

- Utilizzare password robuste, difficili da individuare

Es: password di 8 caratteri

- Alfabeto da 36 simboli (minuscole + cifre)
- 36^8 ~ 2,82 x 10^{12} combinazioni

- Alfabeto da almeno 84 caratteri (maiuscole + minuscole + cifre + 22 caratteri speciali)
- 84^8 ~ 2,47 x 10^{15} combinazioni

Non è necessario cambiarla spesso, ma sceglierla bene!

Proteggere macchine della rete

Password

Misura di sicurezza sottovalutata

Nella nostra esperienza di supporto la quasi totalità delle intrusioni è iniziata con violazione di password semplice

La stessa password usata per un servizio NON critico può essere sfruttata con altri servizi e causare maggiori danni
Es: password di una ibay di test usata per fare spam

Accessi al firewall

Base tecnologica (RHEL) sicura e aggiornata
-> evitare accessi indesiderati dipende dalla configurazione

- Scelta della password robusta
- Limitare accessi amministrativi
    - ssh
    - Interfaccia web (httpd-admin su porta 980)

Accessi al firewall

ssh : modificare porta di default (22)

- non assicura inviolabilità
- diminuisce numero di attacchi medio
- riduce log di tentativi di attacco

nethesis

Accessi al firewall

ssh e httpd-admin : consentire accesso solo a reti fidate (tipicamente la propria rete pubblica)

Menu: Sicurezza-> Servizi di rete

httpd (HTTP)	TCP: 80,443	ACCEPT: green, red	Modifica
httpd-admin (Interfaccia web NethServer)	TCP: 980	ACCEPT: green, red	Modifica
mysqld (Database MySQL)	TCP: 3306	ACCEPT: localhost	Modifica
ntopng (Analizzatore traffico di rete)	TCP: 3000	ACCEPT: green	Modifica
nut-server	TCP: 3493	ACCEPT: green	Modifica
openvpn@host-to-net	UDP: 1194	ACCEPT: green, red	Modifica
snmpd (SNMP)	UDP: 161	ACCEPT: green	Modifica
squid (Proxy web)	TCP: 3128,3129,3130	ACCEPT: green	Modifica
sshd (Secure Shell)	TCP: 222	ACCEPT: green, red	Modifica

Accessi al firewall

Come operare

- Regola di firewall che consente accesso da reti pubbliche fidate
- Disabilitare accesso RED su ssh e httpd-admin

nethesis

Accessi al firewall: abilitare accesso dall propria rete

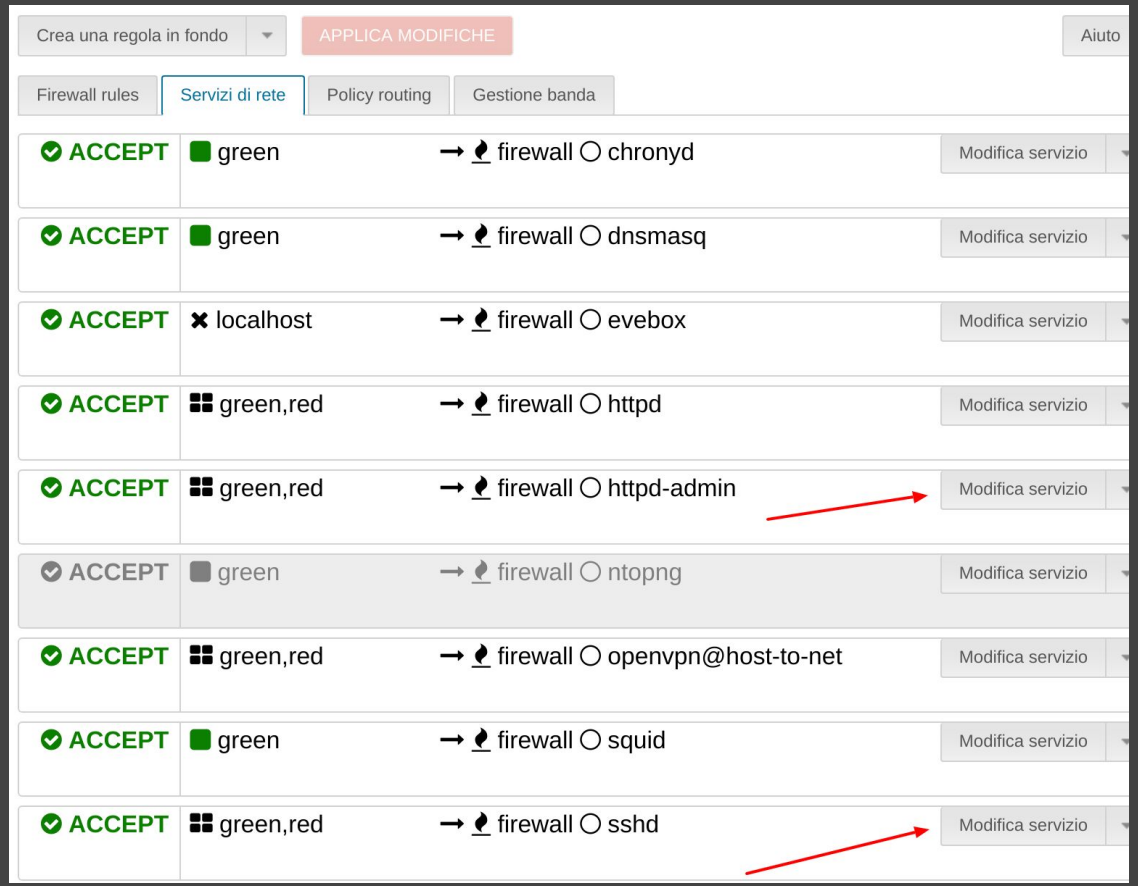
nethesis

Accessi al firewall: abilitare accesso dall propria rete

nethesis

Accessi al firewall

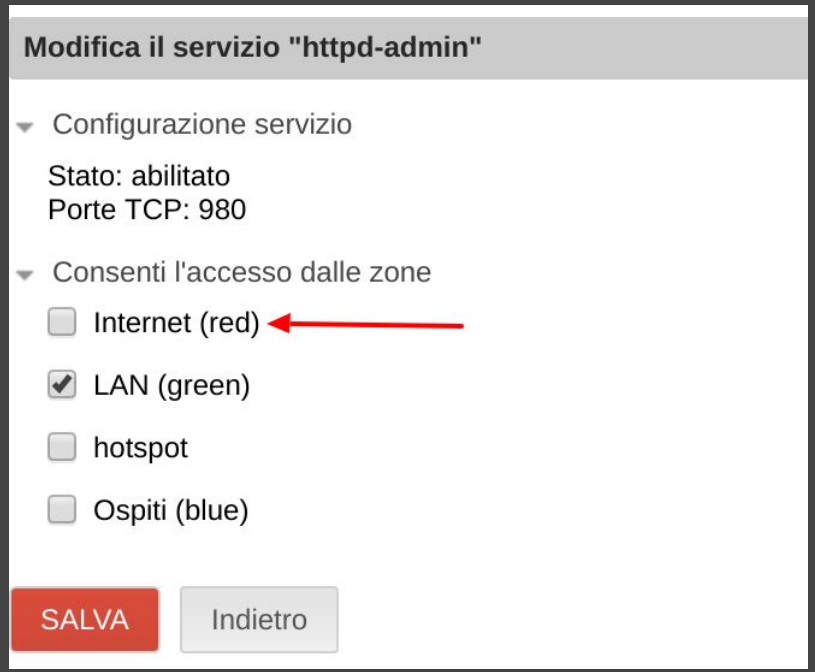
Disabilitare accesso da red



nethesis

Accessi al firewall

Disabilitare accesso da red



Server esposti pubblicamente (port forward)

I server esposti pubblicamente a maggior ragione devono essere aggiornati e protetti adeguatamente

Tipicamente port forward usati per accessi da parte di esterni

- Crearli se necessario/rimuoverli quando non più utili
- Limitarli per IP quando possibile
- Evitarli su macchine che non possono garantire

Livelli di sicurezza adeguati

es: telecamere IP, citofoni, altri apparati *particolari*

VPN

Tipicamente utilizzate per accesso di utenti *aziendali*

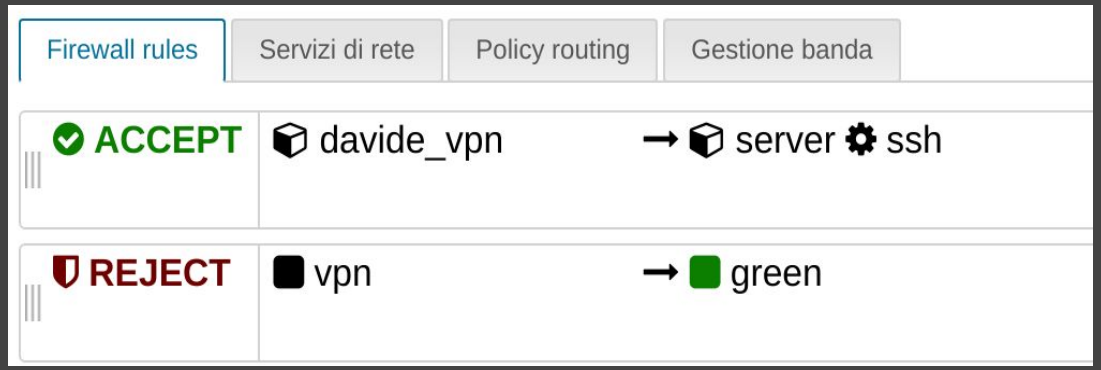
- Accesso alla intera rete
- Utilizzare VPN per accedere a telecamere IP o altri apparati se non è possibile limitare il port forward
- Non è sbagliato limitare accesso alle sole macchine che devono essere accessibili da remoto

Se VPN utilizzate per utenti ***esterni*** all'azienda è caldamente consigliato limitare l'operatività alle sole macchine e servizi necessari

nethesis

VPN : Creazione regole di firewall

- Associazione account VPN -> indirizzo IP
- Creazione oggetto host con lo stesso indirizzo IP
- Creazione di regole di firewall sull'indirizzo IP definito



IPS: Intrusion Detection and Prevention System

- Analisi di tutto il traffico che attraversa il firewall
- Azioni su minacce
  - Alert
  - Block
- Impatto sulla rete: può bloccare traffico legittimo

IPS : Intrusion Detection and Prevention System

Block sicuro:

- ET-botcc.portgrouped
- ET-botcc
- ET-ciarmy
- ET-compromised
- ET-drop
- ET-dshield

Block nella maggior parte delle reti:

- ET-emerging-activex
- ET-emerging-attack_response
- ET-emerging-dos
- ET-emerging-exploit
- ET-emerging-malware
- ET-emerging-netbios

Alert:

- Categorie rimanenti

TLS Policy

- Politiche di sicurezza più restrittive
- Di default sulle nuove installazioni 7.5 NG

- A breve nuovi default più restrittivi anche su VPN

Privacy

- ntopng in ascolto solo su localhost

httpd-admin (Interfaccia web NethServer)	TCP: 980	ACCEPT: green, red	Modifica
mysqld (Database MySQL)	TCP: 3306	ACCEPT: localhost	Modifica
ntopng (Analizzatore traffico di rete)	TCP: 3000	ACCEPT: localhost	Modifica

Solo l'admin può visualizzare ntopng

Ulteriori misure: Traffico bloccato in uscita di default

Misura proporzionata al contesto

- Consentito traffico in uscita per servizi indispensabili
- Tutto il traffico rimanente bloccato
- Già presenti su *oggetti firewall* gruppi di servizi (navigazione, email) per consentire una rapida implementazione

dns	tcpudp	53
email-grp	tcp	25,110,143,465,587,993,995

telnets	tcpudp	992
web-grp	tcp	80,443,980

Domande?

Grazie per l'attenzione