Presentazione questionario Gestione dispositivi degli utenti

Tutorial days di CCR: Cybersicurezza

10-12 Ottobre 2022

Paolo Veronesi (INFN-BOLOGNA)

Premessa

Il 29 Luglio è stato inviato il Questionario destinato ai Servizi Calcolo e Reti delle sedi – Per TUTORIAL DAYS

4 ambiti di domande relative alla cybersecurity. Finalizzate a conoscere meglio le soluzioni adottate nelle sedi ed a presentarle, discuterle, approfondirle durante i Tutorial Days 2022 (10-12 ottobre a Frascati)

Risposte da 23 sedi INFN

Gestione dispositivi degli utenti

- Gli utenti hanno in dotazione pc/laptop acquistati dall'ente e spesso usano anche propri dispositivi personali (pc/laptop/smartphone), soprattutto da remoto.
- Per quel che riguarda il mondo wifi, è consolidato l'uso di INFN-Dot1x e Eduroam, per cui l'autenticazione avviene a livello utente.
- Per quel che riguarda la connettività via cavo, la situazione è più variegata. Spesso gli utenti richiedono la registrazione del MAC address del loro dispositivo e questo viene autorizzato a ricevere un ip quando connesso. La presenza di adattatori ethernet via usb (tipica del mondo apple, ma non solo) complica ulteriormente il poter risalire la catena completa (MAC address - dispositivo - utente).
- Le seguenti domande hanno lo scopo di raccogliere informazioni su come vengono gestiti i dispositivi personali degli utenti sui quali gli utenti hanno solitamente privilegi amministrativi.

In questi BOX trovate qualche mio commento

In questi BOX segnalo i tutorial derivati dalle risposte del questionario

15.Come avviene la registrazione di un dispositivo (pc/laptop) sulla rete via cavo? (1/2)

3	MAC address - DHCP

12	• Tramite form online, protetta da login AAI
	• Richiesta scritta (email) al Servizio di Calcolo in genere alla accettazione AUP
	• L'utente fa una richiesta via mail a calcolo
	  • Se la richiesta è lecita gli assegnamo un indirzzo IP da una classe privata (172.16.x.x) e memorizziamo sul nostro DNS interno l'assegnazione (ip/nome della persona/indirizzo mail/data di assegnazione).
	  • Se il dispositivo è un PC fisso l'indirizzo IP viene configurato manualmente.
	  • Se è un laptop (o adattaore usb) registriamo anche il MAC address e l'indirizzo IP assegnato viene passato al dispositvo via DHCP.
	• con modulo di richiesta che deve essere stampato e firmato dal richiedente. La richiesta finisce in un database ricercabile per richiedente, indirizzo, data e fqdn richiesto
	• gli utenti richiedono la registrazione del MAC address del loro dispositivo tramite una form. il mac address viene registrato nel DHCP in modo da collegate l'utente al mac address e all'ip che viene associato al mac address.
	• L'utente apre un ticket al servizio calcolo via web
	• Il servizio calcolo utilizza un tool web based per la registrazione dei MAC address, la generazione dei file di configurazione del DHCP e del DNS. L'utente invia una richiesta in fase di apertura di una nuova utenza con il mac address dei dispositivi; in seguito via mail le richieste di nuovi mac address o cancellazioni vecchi device. Un MAC address non registrato NON accede alla rete.
	• Invio del mac via mail ed inserimento su dhcp
	• L'utente richiede via form (protetto da AAI) la registrazione inviando alcuni dati tra cui il mac address
	• Attraverso la registrazione del MAC address via apposito form.
	• La richiesta viene inoltrata via form-web dopo login via identità digitale INFN
	• dietro richiesta via email possibilmente del responsabile del richiedente, con l'indicazione del mac da autorizzare

1	non viene eseguita una preregistrazione del dispositivo (la rete è di proprietà e viene gestita dall'Università ospitante)

15.Come avviene la registrazione di un dispositivo (pc/laptop) sulla rete via cavo? (2/2)

1	gli utenti che hanno un account locale possono registrare il mac-address di questo dispositivo. Questo permette l'accesso via DHCP alla rete cablata e l'accesso ad una rete WiFi interna. Gli utenti che si autenticano con eduroam e INFN-Dot1X invece sono considerati esterni.
1	autoregistrazione con username INFN-AAI via INFN-Dot1x
1	I dispositivi non vengono preventivamente registrati. L'associazione tra un utente e un dispositivo viene fatta dagli strumenti di autenticazione e discovery attivo di indirizzi MAC e IP.
1	Registrazione del MAC: le informazioni sono raccolte direttamente dal personale del Servizio per i sistemi acquistati dall'ente oppure forniti dall'utente attraverso il sistema di ticketing Jira con un form preimpostato. In entrambi i casi le informazioni vanno ad alimentare un DB degli asset.
1	Tramite un'interfaccia web -> db -> radius server. L'accesso è riservato al servizio calcolo.
1	laptop lavora wifi su INFN-dot1x. Ai pc vengono assegnati un ip fisso, via dhcp.
1	Stiamo mandando in produzione (fine Settembre) un sistema basato su fortigate e con app sviluppata ad hoc, che permette la registrazione di mac address usando il login AAI su un database alimenta poi le regole del firewall.

Tutorial su Packetfence

- La maggior parte prevede richiesta (autenticata via AAI) a gruppo calcolo e reti che poi agisce manualmente su dns/dhcp. Questo scenario è un'ottimo candidato ad essere automatizzato
- Alcune informazioni per legare utente/mac address/ip sono salvate in posti non proprio appropriati come commenti => necessità di un DB degli asset

16. Possono essere registrati via cavo solo dispositivi acquistati dall'ente o anche personali?

4	• Acquistati dall'INFN o dal Dipartimento • non capita mai di registrare dispositivi personali su cavo • La policy e' di non registrare pc/laptop personali alla rete INFN via cavo. • Solo dall'Ente (ci sono state eccezioni per i personali ma sono molto limitate)

16	• Anche personali, importante specie in caso di ospiti.
	• anche personali o del dipartimento
	• Anche personali è prevista una VLAN Ospiti dedicata non ancora attivata.
	• Registriamo anche dispositivi personali se la persona è autorizzata all'utilizzo delle risorse IT dell'ente cioè se rispetta questi 3 punti:
	  • è dipendente/associato (o autorizzato dal direttore)
	  • ha accettato il disciplinare
	  • ha fatto il corso sulla sicurezza

2	• non abbiamo modo di sapere la provenienza dei dispositivi per i quali ci viene richiesto il collegamento alla rete • Anche personali, non avremmo modo di fare enforcing.
1	la rete è di proprietà e viene gestita dall'Università ospitante

- Nel nostro ambiente è comune, se non indispensabile, registrare anche dispositivi personali o di non dipendenti
- E' importante che il processo di registrazione (manuale o automatico) preveda la verifica dei requisiti via AAI

17. C’è un limite temporale di validità della registrazione dopo il quale la richiesta va risottomessa?

19	• No (buona idea per il deprovisioning automatico) • Nessun limite, tranne la validità della registrazione dell’utente stesso. • No, non stringente. Verifichiamo periodicamente se i dispositivi registrati non esistono più o se la persona di riferimento ha lasciato la sede. • La registrazione scade alla scadenza dell'account personale • le richieste di indirizzo temporaneo hanno la loro naturale scadenza, quelle a tempo indeterminato no. • no, periodicamente si procede alla rimozione di quelle non necessarie • Fino a che il dispositivo e' inventariato rimane registrato. Un software di sniffing della rete ci notifica i device che non sono utilizzati da piu' di un certo tempo. • Sulla rete cablata i mac address che non accedono alla rete dopo un anno vengono cancellati dal tool di gestione della rete • Alla scadenza dell'associazione + 30 giorni viene tolta l'autorizzazione • Un anno per gli ip dinamici. Dopo, non è garantito l'accesso (periodicamente puliamo le liste di ip disconnessi da tempo)
3	• dopo 12 ore è necessaria una nuova autenticazione via credenziali • Si • Chi non registra il proprio mac address sull'app dedicata viene rimandato al captive portal del fortigate: il tempo di memorizzazione del device è di 30 giorni - limite massimo dato dal fortigate stesso
1	la rete è di proprietà e viene gestita dall'Università ospitante

Si sta sempre parlando di dispositivi assegnati agli utenti, single user (il desktop/laptop da scrivania per intenderci)
E’ importante anche che le registrazioni siano temporanee (un utente cambia dispositivo, un associato termina di esserlo, etc), ma senza creare eccessivo disagio agli utenti.

18.C’è un limite nel numero dei device personali che possono essere registrati?

18	No
3	• No, ma uno solo di questi viene considerato dispositivo principale con numero IP fisso • No, non abbiamo mai avuto abusi • no, si usa buon senso
1	Zero
1	la rete è di proprietà e viene gestita dall'Università ospitante

Non essendoci un limite al numero di device per utente che possono essere connessi via cavo, è importante che i processi di registrazione e rimozione del dispositivo siano automatizzati e le registrazioni abbiano una durata limitata

19. Viene assegnato un ip dinamico o statico o a seconda dei casi (es dinamico per i portatili, statico per i desktop)?

8	• Statico per tutti, tranne che per eduroam/INFN-dot1x • Statico per IP standard e dinamico con DHCP • statico sia per i portatili che per i desktop • Tutti gli IP sono forniti attraverso il dhcp in maniera statica (associazione IP - mac address) • Statico per tutte le macchine di servizio (assegnate all'utente dall'Ente) • Sempre indirizzo statico sulla rete cablata per desktop e portatili (indirizzo dinamico sulla rete wireless).
9	• I PC desktop hanno sempre un IP fisso/statico. I PC portatili invece hanno un IP dinamico a parte un PC chiamato principale che lo puo' avere statico. • l'indirizzo IP assegnato è fisso ma viene configurato staticamente o dinamicamente (via dhcp) a seconda del tipo di dispositivo (statico per i desktop, dinamico per i laptop) • Dinamico per i portatili e statico per i desktop, ma gestito comunque via DHCP. • Solitamente dinamico per portatili, fisso per desktop • Dinamico per i portatili, di norma statico per qualche desktop (le eccezioni riguardano dispositivi che non necessitano di essere contattati - questi acquisiscono indirizzi stabili in rete privata)
2	• la scelta e' demandata al richiedente
3	• Dinamico • ip dinamico per PC sia portatili che desktop, ip fisso per stampanti

Lo scenario è che i dispositivi degli utenti (laptop/desktop da scrivania per intenderci) tendenzialmente non hanno bisogno di un ip fisso, la domanda era un po’ malposta.
Soprattutto nel caso in cui l’ip non sia fisso, occorre tenere traccia delle varie assegnazioni per un certo periodo di tempo

20.Come vengono gestiti gli adattatori usb2ethernet?

18	• Come le normali schede di rete • come per i laptop • Anche questi vengono registrati come i portatile in modo tale che siano sempre associabili ad un utente (anche se magari gli utenti se lo passano, ma questo succede anche per i portatili) • Allo stesso modo di una macchina fisica. • Docking station e adattatori , se acquistati INFN, vengono registrati e associati ad un utente.
2	Al momento non li gestiamo
1	non avendo un meccanismo di autenticazione basato su mac address il convertitore puo' passare da computer ad un altro senza alcun problema
1	Si impone nella configurazione del BIOS il MAC Passthrough (per i Lenovo) gli adattatori Dell si comportano già così. I Mac sono un problema.

Qui emergono diverse problematiche che riguardano l'identificazione dei dispositivi (attraverso il MAC ADDRESS) vs l'identificazione dell'utente che usa un determinato dispositivo

21. I dispositivi acquistati dall'ente e assegnati agli utenti vengono gestiti via un sistema di asset management? Quale?

5	• In corso di completamento la configurazione di **inSight di Atlassian** JSM • **Insight** • Tutti i dispositivi registrati sono inseriti nel database di **NetQuery**, il nostro sistema di gestione della rete, che funge pertanto anche da asset management per le device registrate. • e' stata effettuata una sperimentazione con **Spiceworks** sui pc degli amministrativi e sugli apparati di rete • **OpenDCIM** (In fase di adozione)
3	• Un **sistema sviluppato ad hoc**. • Tutte le macchine registrate in rete (anche quelle personali) vengono inserite in un DB degli asset attraverso un **tool sviluppato in casa** in Visual Basic con MySQL come back-end. • Abbiamo un **database dell'hardware autoprodotto** in cui nella scheda del dispositivo viene inserito il seriale e il numero d'inventario.
3	• No, utilizziamo i file di testo del DNS dove teniamo le informazioni rilevanti. • Per ora il sistema e' manuale e basato sui dati registrati in DNS, dhcp, puppet confrontati con il sistema di sniffing della rete • Non viene usato un tool di asset management specifico, ma le richieste di registrazione dei dispositivi sono tracciate via ticket.
11	• No • Sarebbe bello, ma non abbiamo le risorse (in termini di manpower) per farlo.

- Quella sull'asset management è un'attività che merita di essere affrontata in ambito CCR
- Occorre tenere conto dei diversi use case tra sezioni e laboratori
- Come asset si pensa spesso solo all'hardware, ma anche il software è un asset
- Automazione quando possibili: ci sono diversi agent OSS disponibili (es FusionInventory, OCS inventory, ma anche il sempre verde SMNP)

Parliamo di asset management

22.E' prevista una verifica sulla effettiva installazione dell'antivirus ufficiale INFN?

	• Si, solo per RUP • Si per i dispositivi GA, per gli altri è responsabilità dei singoli utenti • No, ma i PC Windows vengono gestiti quasi tutti centralmente. Nel modulo di registrazione l'utente si impegna ad installare l'antivirus ma non c'e' enforcement • La verifica e' eseguita all'atto della registrazione dell'indirizzo IP, non e' automatica. • No • È richiesta l'installazione dell'antivirus ufficiale dell'ente, ma non c'è un sistema di verifica automatizzato. • Non automatica, si cerca di 'sensibilizzare' gli utenti in particolare gli quelli Mac (senza grande successo). • NO. Gli utenti vengono invitati ad installare l'AV ufficiale e sono supportati nell'installazione/disinstallazione, ma non c'e' una verifica. Teniamo presente che sulla rete cablata o wireless sono presenti laptop di colleghi di altre sedi INFN o di altri entri in turno per gli esperimenti e su questi non facciamo nessuna verifica e non diamo supporto.

- C'è attenzione per dispositivi gestiti dai servizi calcolo (in particolare i GA)
- Si invitano gli utenti a seguire il «**disciplinare uso delle risorse informatiche**» e le «**norme di uso dei vari sistemi operativi**»
  - Qualche difficoltà in più con chi usa MacOs

23. Viene usata una VPN per l'accesso da remoto alla LAN della sezione? Se sì, ci sono policy particolari applicate? (es, sono accedibili tutti i servizi di sezione come se l'utente fosse in ufficio o ci sono limitazioni)

- 2 VPN. Una per tutti gli utenti, una per l'accesso alle network di management (per i soli sistemisti)
- Si, con VLSn dedicata e raggiungibilità totale della LAN di Dipartimento senza filtri particolari, come se l'utente fosse in ufficio.
- Sì utilizziamo OpenVPN con split-tunnel. Sono raggiungibili, per default, via vpn solo le classi IP della rete cablata. Solo alcuni power-users (ad es. i membri del servizio calcolo) possono raggiungere via vpn tutte le reti, incluse quelle di managemet a cui sono collegati i dispositivi più critici.
- L'utente puo' scegliere di utilizzare una VPN che da accesso a tutto, anche ai siti non dell'Ente, oppure utilizzare una VPN Split tunnel che da accesso ai soli servizi della Sezione (tutti)
- Si, si sono accessibili tutti i servizi locali di rete pubblica e delle reti nascoste
- È disponibili un servizio di VPN che dà accesso a tutti i servizi di sezione come se si fosse all'interno della rete della sede. Gli appartenenti ai Servizi di Direzione e Amministrazione utilizzano una VPN separata con un elenco di indirizzi IP relativi ai servizi INFN: solo il traffico diretto a questi IP passa attraverso la VPN, mentre il resto del traffico no.
- Si, ci sono due tipi di accesso, quello diretto e con NAT, l'accesso diretto pone il dispositivo remoto direttamente sulla LAN è utilizzato dal personale dell'amministrazione e direzione per motivi di supporto da parte del servizio calcolo che in caso di problemi può effettuare un'assistenza remota o attivare un remote desktop. Quello con NAT pone i dispositivi in una rete privata che utilizza un unico IP pubblico sulla LAN.
- Si, la LAN e' segmentata e la VPN permette di indirizzare gli utenti al segmento di loro pertinenza

- Si scoraggia l'uso della VPN. Se la usano non ci sono restrizioni. Si preferisce SSH Tunnel

- Split tunnel e/o full
- Pochi usano diverse VPN per reti diverse o con limitazioni legate all'utente
- VPN vs SSH Tunnel
- Autenticazione locale vs AAI
- OpenVPN va per la maggiore

24.E’ possibile per gli utenti collegarsi via Remote Desktop ai propri dispositivi in sezione? Se sì, solo via vpn o liberamente?

20	• Solo via vpn • Sì, il "remote desktop" inteso come windows/RDP è acccessibile solo da VPN. Non blocchiamo altri tool di accesso remoto per i quali non è necessaria VPN (ad es. TeamViewer). Il servizio calcolo e reti verifica comunque che sulle macchine GA questi tool non siano presenti. • Chi non e' admin del proprio PC windows deve chiedere al servizio calcolo di abilitare l'accesso via remote desktop. Chi vuole accedere tramite VPN deve chiedere un account sulla VPN. Non e' possibile un accesso diretto ma solo tramite bastion host, con un tunnel SSH
1	• liberamente
1	• No

L’accesso via tool di desktop remoto va approfondito

- Attenzione al software licenziato, ma libero per uso personale
- Attenzione a come funzionano questi software, spesso passano da siti terzi

Tutorial su AnyDESK / tool per il supporto remoto

25.Viene dato supporto alla configurazione di smartphone/tablet degli utenti?

13	• Abbiamo scritto istruzioni, ogni tanto ci tocca dare supporto, ma non lo facciamo ad altissima priorità • Supporto limitato • No, ma gli utenti a volte lo chiedono e se vogliono accedere alla posta cerchiamo di aiutarli. Best Effort • su base volontaria • Sì, in maniera best-effort. • si, per la parte di accesso in rete • Per configurare eduroam e l'accesso all'email. • best effort, ma capita raramente • Solo per posta e wifi
3	• Si • Si, a malavoglia..
6	• No • No, a meno che non sia device inventariati INFN / Dipartimento. • in generale no

A mio parere sono da tenere sotto osservazione

Spesso parliamo di dispositivi personali che niente hanno a che fare con il lavoro

- Su questi dispositivi gli utenti installano le app più svariate
- Ha senso che gli smartphone si colleghino a dot1x?

Esperienza personale: ho android vecchio (cellulare di 4 anni), openvpn, un client ssh, la posta configurata, mi collego con eduroam.

- Openvpn e client ssh usati raramente, la posta spesso

26.Gli utenti sono amministratori dei loro dispositivi (smartphone/tablet)?

22	• Si • si di norma lo sono. Altrimenti avrebbero difficolta' ad usarli da casa, da altre sedi o dai laboratori • Sì per i dispositivi personali, i laptop (anche se di proprietà dell'ente) e le macchine con funzioni speciali come ad esempio quelle di laboratorio/DAQ. • Sono device personali. • I dispositive lavorativi sono assegnati a persone specifiche. I tablet acquistati per controllare I green pass sono in gestione al servizio calcolo e reti

Smartphone e soprattutto tablet stanno diventando strumenti lavorativi in particolare ambiti.
L’impressione è che non ci sia la stessa attenzione che si ha per i portatili (es: antivirus?)

27. Cosa pensi della possibilità di installare un agent sui laptop/desktop degli utenti al fine di avere un sistema di asset management e fare alcune verifiche (es aggiornamenti s.o., antivirus, etc).

23	• Ottima idea • Favorevole per sistemi critici, come quelli dell'Amministrazione, mentre per gli altri potrebbe risultare invasivo. • Sarebbe sicuramente una buona idea per tutti i dispositivi GA. Per quelli TS mi sembra uno scenario non realistico. • mi sembra una buona idea ma e' lavoro iu piu' sui servizi calcolo • Dipende se poi questo mi rendesse poi amministratore di sistema con gli obblighi del caso. Se la cosa mi dovesse rendere amministratore, me ne guarderei bene dall'installarlo perche' so benissimo che non avrei comunque modo di mettere in pratica delle buone pratiche di gestione della macchina e ne sarei comunque responsabile anche penalmente. Sui pc degli amministrativi dove sono gia' amministratore non avrei problemi a farlo, anzi... • dipende dalla facilita' di configurazione e dalle necessita' di manutenzione dell'agent. L'ideale secondo me sarebbe associarlo all'AV stesso, evitando il proliferare di agents • Dovrebbe essere disponibile per ogni S.O. • Non penso sia realmente possibile fare un enforcing

- Accordo di massima per i sistemi GA
- In generale, da capire se applicabile a tutti i dispositivi acquistati dall'ente (per motivi inventariali e non per security)

28. Per il Lavoro “Agile” in sezione, agli utenti sono stati forniti dispositivi aggiuntivi? Gli utenti utilizzano (o possono utilizzare) dispositivi propri quando sono in lavoro “agile”?

21	• Tutti hanno un dispositivo portatile • Dal primo lockdown ad oggi c'è stato sicuramete un incremento dei dispositivi mobili forniti dall'ente al personale in smart working. • Gli utenti utilizzano comunque anche i propri dispositivi. • Sono stati dati notebook per il lavoro agile in periodo di pandemia. Nei primi periodi molti usavano il loro dispositivo. • sono stati dotati di dispositivi aggiuntivi • Il personale di Amministrazione e Direzione è dotato solo di laptop, per cui usa sempre la stessa postazione sia in ufficio che in lavoro agile; il resto degli utenti può utilizzare anche dispositivi propri. • Sono stati forniti dispositivi aggiuntivi. Non devono usare dispositivi propri. • Per il telelavoro agli utenti interessati sono stati forniti dispositivi di proprieta' dell'istituto. Non so se ci sono dipendenti in lavoro agile al di fuori di questi casi (il lavoro agile si applica solo ai livelli IV-VIII) Per il lavoro fuori sede dei livelli I-III non c'e' alcun modo di controllare, e' possibile che vengano utilizzati dispositivi personali (io sto rispondendo al presente questionario fuori
2	• No • No, e viene raccomandato di non utilizzare dispositivi personali.

- In generale, aumento nell’ente di soluzioni desktop replacement (solo portatile + docking + monitor/tastiera e mouse esterni)
- Telelavoro vs lavoro agile vs lavoro fuori sede
- Ritorna il tema dei dispositivi personali permessi e non

Conclusioni

Grazie per aver compilato il questionario!

- In questa edizione dei Tutorial Days abbiamo estrapolato dalle risposte e preparato come tutorial quegli argomenti che per interesse e tempistiche meglio si concigliavano con il formato dell'evento e con la disponibilità degli speaker (che ringrazio) cercando di privilegiare la formazione sull'informazione.
- Diverse risposte mettono in luce approcci diversi a problematiche comuni e credo che già di per se possano accendere interesse nelle varie sedi INFN
  - Forse manca un posto dove condividere queste esperienze, questo evento può essere un punto di partenza come repository