Presentazione questionario Supporto all'amministrazione

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

Supporto all’amministrazione

Tra i compiti specifici del servizio calcolo e reti vi è quello del supporto informatico agli uffici del personale e dell'amministrazione locali. Le seguenti domande hanno lo scopo di raccogliere informazioni ed esperienze sul supporto informatico dato dal servizio Calcolo e Reti all’Ufficio Personale e Amministrativo.

In questi BOX trovate qualche mio commento

In questi BOX segnalo i tutorial derivati dalle risposte del questionario

1. **Gli afferenti dell'ufficio del personale e dell'amministrazione della tua sede hanno utenze privilegiate sui rispettivi dispositivi di lavoro?**
   - 21 no
   - 1 si

2. **I pc/laptop dell'ufficio del personale e dell'amministrazione sono gestiti dal servizio calcolo con utenze amministrative personali o con Administrator?**

utenze amministrative personali	7
Si	5
Con una utenza amministrativa unica / come amministratore del dominio	6
Administrator i pc personali non oggetto di misure minime, utenze amministrative personali sul server oggetto di misure minime	1
Ove possibile con utenze personali con privilegi amministrativi	1
Entrambe	2

L'impressione è che non ci sia un problema tecnico, solo una abitudine a non utilizzare account personali distinti tra utente e administrator.
Es: per Bologna, in Active Directory, pveronesi (utente) e pveronesi2 (administrator). Manca questa possibilità in AAI

3. Quali sistemi operativi sono usati?

2	macOs
6	Mac / windows
15	Windows 10 / W10/W11; Windows 10 LTSC; W2012R2/ Windows 10 Pro/Enterprise

- Niente linux (in generale poco o niente Open source software (OSS))
- Controllo di cosa e quando viene aggiornato e automazione nell'aggiornamento
- Mia esperienza: Windows update automatico ha minimi effetti collaterali

4. Come viene aggiornato il sistema operativo?

1	Manualmente (Mac)
3	Windows update e Manualmente (Mac)
3	Manualmente (Windows e Mac)
1	Tramite WSUS a tutti, ma dopo test su alcuni pc cavia
1	Windows update automatico e manualmente sui windows server
9	Windows update
2	Aggiornamenti di Windows con Windows Update automatizzati e programmati con i criteri di gruppo distribuiti dal domain controller.
1	Gli aggiornamenti vengono effettuati manualmente dal personale del servizio calcolo o da una persona del servizio esterno "gestione postazione di lavoro" autorizzato al trattamento dei dati personali.
1	in automatico o tramite intervento di manutenzione da parte del servizio calcolo in media una volta al mese
1	windows update, in alcuni casi occorre procedere manualmente, in altri gli aggiornamenti vengono applicati automaticamente

5. Come vengono aggiornati gli applicativi (es firefox)?

9	Manualmente
1	alcuni si aggiornano automaticamente, altri su richiesta degli utenti.
1	**Chocolatey** sui pc degli amministrativi e a mano sul terminal server
1	**Chocolatey task update** allo startup (non sempre funziona) - Manualmente dal servizio calcolo.
1	dall'utente stesso se l'aggiornamento lo prevede altrimenti dal servizio di calcolo
1	La maggior parte degli applicativi supporta gli aggiornamenti automatici. Nel caso non fosse possibile, interviene uno degli amministratori manualmente. In corso studio su come automatizzare gli aggiornamenti considerati sicuri (idealmente **Puppet + Chocolatey**).
1	Task Amministrativo
1	Alcune tramite group policy (dove supportato) altre con interventi puntuali
1	**Puppet + chocolatey**
1	Gli aggiornamenti vengono effettuati manualmente dal personale del servizio calcolo o da una persona del servizio esterno "gestione postazione di lavoro" autorizzato al trattamento dei dati personali.
2	Alcuni applicativi (ms office, adobe) sono automatici. Altri sono aggiornati dal servizio calcolo "quando serve".
2	Dal servizio calcolo dopo la segnalazione da parte dell'utente

Tutorial Chocolatey - packet manager per Windows

Nel 2023 è previsto un evento formative su Foreman/Puppet/Ansible che comprenderà anche un talk su Puppet/Chocolatey

Mia esperienza: l'aggiornamento automatico degli applicativi (non disattivabile dall'utente) ha minimi effetti collaterali

6. I dispositivi dell'ufficio del personale e dell'amministrazione sono su una rete dedicata, o vengono usate delle policy di rete particolari per i dispositivi?

9	No
1	VLAN dedicata con filtri dedicati per restringere gli accessi
1	sono in un range dedicato con regole di confinamento. Vengono periodicamente controllati per vedere se ci sono nuovi applicativi o nuove versioni di applicativi gia' installate. Vengono sottoposte a scansioni periodiche con GreenBone
1	I dispositivi non sono su rete dedicata, mentre il terminal server dove risiedono applicativi e dati soggetti alle misure minime e' accessibile esclusivamente via LAN oppure VPN (e' filtrato sul router)
2	sono su rete nascosta come tutti i pc di Sezione, non è stata creata una rete dedicata all'amministrazione
1	La rete degli utenti in questione è gestita su uno spazio di indirizzamento IP dedicato su una VLAN separata dalla rete standard di Sezione.
1	LAN di laboratorio, condivisa con altri utenti.
1	Sono sulla rete dei desktop di dominio windows
1	Ci sono policy sul traffico inbound/outbound
1	L'amministrazione e' su un ramo di rete dedicata, protetta da fw. I dispositivi della direzione sono sulla VLAN dell'edificio che ospita gli uffici di Direzione.
1	Per il momento no, e' previsto lo spostamento delle macchine su una rete dedicata presidiata da un F/W
3	Rete dedicata. VLAN dedicate.

Il design della rete è un elemento da tenere in considerazione anche per gli aspetti di sicurezza
Sicurezza della rete non solo da attacchi dall'esterno, ma anche interna

- Tutorial su Packetfence
- Tutorial Greenbone/nmap

7. Quale dispositivo di autenticazione viene utilizzato? (es account locali, Active Directory, etc).

11	Account locali
1	Dominio Active Directory gestito da Samba su Linux
1	account locali sui pc degli utenti e server Kerberos centralizzato di autenticazione sul server Windows oggetto di misure minime
1	Gli account degli utenti sono creati via Active Directory e, attraverso un trust tra il dominio Windows e il realm Kerberos della Sezione, utilizzano le credenziali INFN per autenticarsi.
1	AD per i PC in dominio, locale per i portatili.
5	AD
1	Ldap locale
1	Active Directory e account locali
1	i pc fissi sono in un dominio windows, i portatili dispongono di account locali

INFN AAI vs Account locali (in varie salse)

8. È installato/usato un software per il remote desktop? Se sì, quale?

1	Anydesk (per emergenze)
11	Remote Desktop
1	Remotely e Remote Desktop
1	Teamviewer, Anydesk
1	Si utilizzano Connessione **Desktop Remoto** per il controllo remoto e **Assistenza Rapida di Windows** per il supporto interattivo. È installato anche **UltraVNC** per le emergenze, come servizio da attivare manualmente.
1	RDP e Teamviewer
4	No
1	RDP e VNC licenziato sul pc del direttore
1	Anydesk 3 licenze

Attenzione alle licenze
- es Teamviewer NON è utilizzabile in ambito lavorativo senza licenza

Attenzione a come funzionano questi software (alcuni passano da un reflector terzo rispetto)

Tutorial su Anydesk

9. È utilizzato uno strumento di configuration management (es puppet)? Se sì, quale?

16	No
1	stringa di installazione degli applicativi via **chocolatey** sui pc personali, tutto a mano sul server soggetto alle misure minime
2	Group Policy Windows
1	**Puppet (con chocolatey)**
1	**Chocolatey**
1	**Puppet**/Foreman solo sulla parte server.

- Virtualizzazione del servizio Amministrazione
- Tutorial Chocolatey - packet manager per Windows

10. L'installazione da zero del sistema operativo è automatizzata? Se sì, in che modo?

15	No
1	Ci capita raramente di utilizzarla per installare "da zero" un PC perchè tutti quelli nuovi arrivano di solito col sistema operativo preinstallato.
1	viene realizzata manualmente partendo da una immagine preconfigurata
1	Installazione da zero semi-automatizzata utilizzando i Servizi di Distribuzione Windows sul Dominio di Amministrazione e Direzione.
1	PXE + WinPE + **Chocolatey** + script batch
1	Tutti gli utenti amministrativi utilizzano thin client (con installazione minimale standard) che gli permettono di collegarsi via rdp alle proprie virtual machines. Le VM sono create via ansible a partire da template su vmware.
1	Immagine per S.O, **puppet (chocolatey)** per gli applicativi, restore per i dati utente
1	Si usa una chiavetta di installazione standard, senza automatizzazione.

11. Backup: descrivere quale software viene utilizzato, la frequenza, le policy di retention e cosa viene backuppato (1/3)

Nessun backup dei PC. L'area personale è salvata su **AFS** (backup giornaliero). Condivisioni su **OneDrive** non salvate (per ora)
Windows backup e **Time Machine**, più i backup individuali di dati su **NextCloud**. I backup vengono fatti automaticamente con frequenza variabile (normalmente giornaliera). Stiamo controllando ora che tutti i backup siano criptati.
Utilizziamo lo strumento di **backup standard di windows** per creare delle immagini del disco di sistema. Le immagini sono memorizzate su uno share di rete privato che viene messo offline dopo l'esecuzione del backup. Facciamo un backup settimanale e manteniamo i backup delle ultime 4 settimane + 1 backup mensile degli ultimi 4 mesi
Bacula. viene fatto girare ogni notte. Si puo' risalire fino a 3 mesi. Viene backuppato solo le Home degli utenti con una quota. In pratica c:\Users
I pc personali degli utenti non sono oggetto di backup, il terminal server che contiene i dati soggetti alle misure minime ha le aree utente copiate quotidianamente via **SMB** sul disco di un altro pc (pcbackup). 1 volta a settimana questi file vengono trasferiti su nastro assieme ai backup delle altre macchine centrali e i nastri vengono custoditi in un armadio chiuso a chiave in locale accessibile esclusivamente con tessera e log degli accessi. Le aree utente sono anche oggetto di shadow copy sullo stesso disco del server: vengono mantenute 2 versioni dei file delle aree utente (versione del mattino e versione del pomeriggio) che vengono sovrascritte dopo una settimana. Il server con le aree utente e' un server virtuale la cui immagine viene backuppata 2 volte all'anno e messa su disco e su **nastro**

11. Backup: descrivere quale software viene utilizzato, la frequenza, le policy di retention e cosa viene backuppato (2/3)

il sistema completo viene salvato con **clonezilla** su server dedicato una tantum. I files degli utenti vengono sottoposti a backup tramite **owncloud**. I dati su owncloud vengono salvati con policy giornaliere, settimanale e mensili da **Bacula**.
Implementazione di software di **backup Dell** in corso. Al momento l'unico sistema di ridondanza per i dati degli utenti è il funzionamento dei **Profili Roaming** (per i membri di Direzione e Amministrazione).
Utilizzo di **Netbackup** con frequenza giornaliera e retention di sei mesi dello spazio utente sui file server, il backup del disco locale del PC viene svolto a cura dell'utente se lo ritiene necessario.
Viene utilizzato il tool di backup incluso nel NAS (FreeNAS), vedi domanda successiva.
tutto il contenuto della directory INFN viene sincronizzata tramite **syncthing** con un server di backup. Viene fatto un backup giornaliero e settimanale dell'intero contenuto presente sul server di backup. Il backup giornaliero viene mantenuto per 30 giorno. Il backup settimanale viene mantenuto per un anno.
I dati ed i profili roaming (solo desktop, il laptop non ha il profilo roaming) sono mantenuti su share Samba (cluster di due nodi fisici) che vengono salvati attraverso il **tool di backup nativo di Windows** Server. Settimanalmente il backup Full viene salvato su **tape**. La retention e' di un anno.
Dell EMC PowerProtect per VMWare, i thin client non necessitano di backup
time machine, frequenza settimanale, nessun limite di retention, home dell'utente
Sincronizzazione su **owncloud** delle cartelle di lavoro; **bacula** per il backup automatizzato su nastro.
Strumenti di sistema su **dischi removibili** che vengono collegati alle macchine solo durante il backup.
Usato **burp**, frequenza quotidiana, retention 7 giorni, 4 settimane 6 mesi. Vine backuppato lo spazio User
Software **ActiveBackup Synology**. Vengono backuppati giornalmente dischi dati e dischi di sistema. Vengono conservati giornalieri, settimanali, mensili... Retention massima di 12 mesi.

11. Backup: descrivere quale software viene utilizzato, la frequenza, le policy di retention e cosa viene backuppato (3/3)

Per i desktop, si usa **clonezilla**, una volta alla settimana (Wake On Lan e clone automatizzato nel week end). Per i laptop (tutti windows 10) si usano diverse strategie: • **Roaming profile** (in abbandono) • **Punto di ripristino Windows** (utile per problemi sugli update di windows, non impatta solitamente sui dati utente) • **OneDrive** (raccomandato per i file personali) • **Windows Backup**, una volta alla settimana: disco di sistema e dati utente. Abbastanza trasparente lato utente, se il laptop è spento nella data/ora schedulata, il backup salta.
Viene messo a disposizione un server **owncloud** dedicato alla parte amministrativa e del personale. Il server owncloud è sotto backup giornaliero completo, con retention di 3 mesi.
Vengono effettuati backup manuale delle sole directory di lavoro, molto del lavoro viene svolto su sistemi remoti del SI. Il backup vengono effettuati su **HD estern**i archiviati all'interno dei locali dell'Amministrazione
MIcrosoft System Backup, backup dell'intera area utente
viene utilizzato un nas **Synology con proprio client**. viene effettuato un controllo ogni due ore e vengono mantenute le ultime 4 versioni. Viene backuppata solo la cartella dell'utente (C:\users\NomeDellUtente)

11.Backup: qualche considerazione

Il backup merita un approfondimento in altra sede. Alcuni elementi:

- Il metodo di lavoro è fondamentale per ottimizzare il backup
- I dispositivi assegnati agli utenti spesso e volentieri contengono dati personali non lavorativi (musica/foto/video) di notevoli dimensioni
- Lo spazio utente spesso contiene dati di cui non è necessario il backup (cartelle locali imap, cartelle di Cloud storage)
- Distinguere tra:
  - backup dei dati utente (es C:\Users\<username>)
  - backup di sistema (es Windows server vs S.O. pc utente)
  - Disaster recovery
- Ripristino:
  - Ripristino di S.O. automatizzato (via tool di configuration management) e successivo restore dei dati da backup
  - Ripristino full da backup

Shared e Cloud storage (slide successive)

Criptare il backup o non criptare il backup?

- (rarissimi) casi di dipendenti scorretti
- Hacking verso il servizio di backup o shared/Cloud storage
- Privacy dei dati
- Gestione chiave di backup

Backup offline

- Cryptolocker
- Tape o disco
- Retention policy
- Disaster Recovery

- Tutorial su Burp

12. Ci sono directory condivise per gli utenti dell'ufficio del personale e dell'amministrazione? Se si, di che tipo (es samba)

	OneDrive di O365
	NextCloud e Pandora
	istanza locale di Nextcloud. Sui PC degli utenti installiamo il sync client
2	Samba
5	No
	Si
2	Share Windows (AD) con folder per gruppi (Uffici)
	Share Windows (AD) e OwnCloud
	C'e un NAS che esporta le directory di lavoro condivise tra gli utenti
	NAS synology dedicato, su rete dedicata
	Seafile
3	sync 'n share (basato su owncloud)
	owncloud su una istanza di owncloud dedicata ad amministrazione e direzione, non disponibile ad altri utenti e raggiungibile dall'esterno solo tramite VPN
	Alfresco locale e Alfresco Nazionale

13. Viene utilizzato OneDrive (disponibile con Office365) o altro sistema di cloud storage?

11	OneDrive di O365 • più pratico di Alfresco • OneDrive è preinstallato con Windows: si avvisano agli utenti di limitarsi all'utilizzo di dati non personali o strategici per l'ente. Per questi tipi di dati, si consiglia l'utilizzo dei sistemi cloud INFN, quali Pandora e Alfresco. • OneDrive solo per uso sporadico. Owncloud sempre, per sincronizzazione cartelle e condivisione dati. • Possono utilizzare Onedrive o pandora, ma ne viene sconsigliato l'utilizzo per dati "sensibili". • Si raccomanda l'uso di OneDrive per i file personali in modo da limitare il backup ai soli dati di lavoro • OneDrive in modo molto marginale. Owncloud intensivamente.
	NextCloud e Pandora
4	No
7	OwnCloud
	C'e un NAS che esporta le directory di lavoro condivise tra gli utenti
	NAS synology dedicato, su rete dedicata
	Seafile

12. Ci sono directory condivise per gli utenti dell'ufficio del personale e dell'amministrazione? Se si, di che tipo (es samba)
13. Viene utilizzato OneDrive (disponibile con Office365) o altro sistema di cloud storage?

Qualche considerazione.
Anche in questo caso, un metodo di lavoro condiviso e standardizzato è importante

Shared e/o Cloud storage

- Il backup è un effetto collaterale, se l'utente cancella/corrompe un file, questo viene rimosso/corrotto anche dallo Shared/Cloud storage
- L'utente deve mettere i propri file in directory particolari
- Alcuni Cloud storage offrono funzionalità di Cestino, Versioning, Sharing con altri utenti
- Alcune sezioni gestiscono un loro servizio di Cloud Storage

Cloud Storage

- OneDrive
- NextCloud/OwnCloud
- Pandora?

Alfresco

Sharepoint (MS Teams)

- I dati personali – il GDPR
- Tavola rotonda con Gomezel

14. Sono attivi sistemi di sicurezza quali TPM e disco criptato?

9	SI • Tutti i dischi sono cifrati • Siamo in fase di controllo che i dischi siano criptati. • Disco criptato verrà implementato su tutte le macchine GA quest'anno su sollecito dell'audit INFN. • Bitlocker (2) • Opal2 • Si, disco criptato sui portatili non sui desktop. password di protezione sul bios disco di avvio non modificabile. • Si, TPM e disco criptato su portatili di amministrazione e direzione. • Tutti i dischi sono criptati con bitlocker, per i portatili è attivo TPM • TPM e' necessario per alcune funzionalita' di windows10. I dischi sono cifrati con bitlocker
1	Windows 10 no Windows 11 attivato di default.
1	Se i dispositivi supportano TPM lo abilitiamo. Non abbiamo invece casi di dischi criptati.
1	Stiamo facendo il rollout in ambiente di test di vm windows 11 criptate tramite TPM fornito dagli esxi dalla versione 7.x
10	No

Mia esperienza

- Bitlocker su windows (dal 10) non ha problemi (solo quello del salvataggio della chiave, tenuta dal servizio calcolo e reti per il servizio amministrazione)
- TPM ha l'effetto collaterale di non permettere il backup con WakeOnLan + Clonezilla, per questo sui desktop non è abilitato, mentre per i laptop è abilitato
- Con Bitlocker il backup via Clonezilla è di tutto il disco, indipendentemente dallo spazio usato. Dove abilitato, facciamo backup via Windows Backup e non più con Clonezilla)
- Nel caso di un furto di un laptop, la gestione lato DPO è stata agevolata dal fatto di avere TPM e Bitlocker

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