Sec DevOps 2024/2025

Sicurezza di un’azienda

Implementazione delle misure standard di sicurezza all’interno di una startup

Zatelli Tommaso, Fukuhara Bruno, Bota Giulia, Rosi Leonardo, Borrelli Ciro

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	2	S	Implementare ABSC 1.1.1 (Implementare un inventario delle risorse attive) attraverso uno strumento automatico	**AWS Config** - Ogni volta che una risorsa viene creata, modificata o eliminata, AWS Config registra l'evento e lo archivia per un controllo successivo.
1	2	1	S	Implementare il "logging" delle operazioni del server DHCP.	**Amazon CloudWatch Logs** - Acquisizione dei log di rete, inclusi i log DHCP, per monitorare e archiviare le operazioni.
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	**Splunk (CISCO)** - Analisi avanzata dei log per rilevare dispositivi non approvati e aggiornare l'inventario.
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	**AWS Systems Manager** - Scansione automatica dei dispositivi connessi e aggiornamento dell'inventario in tempo reale.
1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	**AWS Asset Inventory**- AWS Asset Inventory non è un servizio AWS specifico con quel nome, ma si riferisce al concetto di gestione degli asset in AWS attraverso vari strumenti che permettono di monitorare e tracciare le risorse presenti nell'account AWS (AWS Config, AWS Systems Manager, AWS Resource Groups, AWS CloudTrail, AWS Security Hub).

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
2	2	1	S	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.	**AppLocker** gestito tramite GPO (Group Policy Objects, se in un dominio AD in AWS) o policy locali configurate tramite **AWS Systems Manager**.
2	2	2	S	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).	Ricorso a **Virtual Machine** con setup dedicato per l'applicazione specifica, e hardening dedicato.
2	3	2	S	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	**Per AWS EC2, AWS Systems Manager Inventory:** è una funzionalità che raccoglie metadati, tra cui anche applicazioni installate. **Per gli endpoint: Microsoft Intune:** un software di gestione degli endpoint, che consente anche l'app listing.

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	2	S	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.	**AWS EC2 Instance Hardening** - offre linee guida per hardening delle istanze EC2, che includono la disabilitazione dei servizi non necessari e la configurazione di sicurezza via Security Groups. xz
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	**AWS CloudFormation** - consente di definire l'infrastruttura come codice, garantendo che tutte le modifiche siano tracciabili e applicate in modo controllato.
3	3	2	S	Le immagini di installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	**AWS EC2 AMIs** - snapshot di macchine virtuali in AWS. Puoi configurare IAM.
3	5	1	S	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	**AWS CloudTrail** - registra le azioni effettuate da un utente o un servizio, compresi eventuali cambiamenti alle risorse e file.

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC_ID			Livello	Descrizione	Modalità di implementazione
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	**AWS Security Hub** - (aggregazione findings)
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	**AWS CloudWatch** + **CloudTrail** – per la raccolta e gestione dei log.
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	**AWS CloudTrail** – registra tutte le chiamate API, incluso l'uso di account scanner.
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	**AWS GuardDuty** – per analisi di attività sospette su asset.
4	3	1	S	Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.	**IAM AWS con policy dedicate** – creare ruolo/utente solo per scanner
4	3	2	S	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.	**AWS Security Groups / NACL** – per limitare l'accesso alle interfacce di scansione.

4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	**AWS Security Hub integrato con feed esterni + Lambda** – per automatizzare l'aggiornamento delle policy di scansione.
4	6	1	S	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	**AWS CloudTrail + AWS Config** – per audit continuo delle attività degli account admin (es. verifica se sono stati usati per funzioni extra).
4	7	2	S	Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.	**AWS Inspector** – con gestione del ciclo di vita del rischio associato a ciascuna CVE (es. tagging "accepted risk", "under mitigation", "remediated").
4	9	1	S	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.	**Security Groups / NACL / IAM** – per isolare rapidamente il servizio vulnerabile o ridurre la superficie di attacco.
4	10	1	S	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	**AWS CloudFormation** – per clonare ambienti con infrastruttura-as-code.

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	**AWS IAM** - Rispettando il principio del least privilege
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	**AWS CloudTrail** - Traccia tutte le chiamate API, comprese operazioni IAM
5	4	2	S	Generare un allarme quando viene aggiunta una utenza amministrativa.	**AWS CloudTrail** - Registra tutte le modifiche IAM
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	**CloudTrail** - Registra tutte le modifiche IAM **CloudWatch Logs** - riceve i log da CloudTrail **CloudWatch Alarms** - Monitora i log e attiva un'allerta **SNS** - Invia la notifica
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	**CloudTrail** - Registra tutte le modifiche IAM
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	**AWS IAM** - Permette di impostare politiche di password per garantire che vengano utilizzate password forti.
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	**IAM** - Configurazione della durata minima per le modifiche alle credenziali.

5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	**IAM** - Per configurare la scadenza delle password e un storico con un periodo minimo di sei mesi per impedire il riutilizzo delle credenziali.
5	8	1	S	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.	**IAM** - Per creare utenti normali e concedere permessi temporanei tramite **AWS STS** per eseguire operazioni privilegiate.
5	9	1	S	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	**AWS Security Groups** - Per applicare restrizioni sugli accessi, assicurandoti che le macchine siano utilizzate solo per operazioni amministrative.
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	**IAM** - Per gestire l'accesso alle risorse in modo centralizzato e disabilitare l'uso di credenziali locali.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	**AWS Cloudwatch Logs** Consente di centralizzare i log di tutti i tuoi sistemi
8	2	1	S	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	**AWS Security Hub** - Monitoraggio continuo della conformità e gestione automatizzata delle policy di sicurezza in AWS.
8	2	2	S	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.	**CrowdStrike Falcon:** Protezione avanzata per Endpoint
8	4	1	S	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	**Data Execution Prevention (DEP) -** tecnologia di protezione che impedisce l'esecuzione di codice da aree di memoria non destinate all'esecuzione (come buffer o stack)..
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	**Windows Defender Firewall:** **Windows Defender Application Guard:**

					AWS Network Firewall **AWS WAF,** per web applications **AWS Shield**, per DDoS prevention
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	**Microsoft Defender for Identity:** consente di proteggere il monitoraggio delle identità nell'intera organizzazione.
8	10	1	S	Utilizzare strumenti anti-malware che sfruttano, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	**Windows Defender Antivirus**:Monitora continuamente file, processi e attività di rete per rilevare comportamenti dannosi **EDR(Microsoft Defender for Endpoint)**
8	11	1	S	Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.	**Azure Sentinel:** Centralizza i log e gli eventi da fonti diverse

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	**AWS Backup** Gestione automatizzata di backup per EC2, EBS, RDS, DynamoDB. Include funzionalità di restore.

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione +
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	**BitLocker (Windows):** Cifra l'intero disco fisico, garantendo che i dati siano protetti anche se il dispositivo viene rubato o perso.(X dispositivi) **AWS Key Management Service (KMS)**: KMS facilita la gestione delle chiavi di cifratura per dati su AWS