Christopher Caruso
Paolo Aglieco
Dario Calderone
Maurizio Pietrangeli
Valentina Arana
Giulio Sorgente
Andrea Molla
Michele Pepe

Calcolo Effort

CIPHER SQUAD

OGGETTO RICHIESTA

Il cliente Theta ingaggia la scrivente società ChipherSquad S.r.l. per attività volte a migliorare il livello di sicurezza della propria infrastruttura

Il perimetro della richiesta è circoscritto alle seguenti attività:

1 Proporre un modello di rete che permetta di garantire i livelli di sicurezza previsti dalle normative vigenti (e.g. GDPR, NIS2) e dagli standard comunemente adottati (e.g. ISO27001, NIST, COBIT). Il modello di rete deve includere un web server esposto e un application server accessibile solo in rete interna

2 Analisi dei servizi attivi sulla macchina tramite port scanning, con evidenza delle relative porte aperte e/o chiuse

3 Enumerazione dei metodi HTTP abilitati sul web server e sull'application server in base al context-path

4 Analisi robustezza della login ad un eventuale attacco bruteforce

Per non generare impatti sull' ambiente di produzione è stato ricreato un laboratorio di test in house con due appliance sui quali sono stati caricati i backup delle macchine del cliente.

ATTIVITA' MITIGATIVE E CALCOLO EFFORT

In questa sezione vengono proposte le attività mitigative inerenti alle criticità riscontrate.
Vengono inoltre fornite indicazioni sull'effort per ogni attività calcolato in ore/uomo.

Port scanning e servizi attivi
1) Chiudere sul web server le porte che non espongono un servizio core relativo al suo funzionamento (e.g. tutte le porte UDP sono aperte ma non espongono servizi) - FTE 1 (1day)
2) Possibilmente effettuare un NAT delle porte rispetto ai servizi di default e preferibilmente abilitare solo canali cifrati (FTPS, SMTPS, etc.) per evitare sniffing del traffico (e.g. risulta aperta la porta 25 SMTP) - FTE 1 (2days)

Robustezza delle password e sistemi di autenticazione
1) Scegliere password con un livello di complessità superiore (e.g. min. 8 caratteri, min. 1 cifra, maiuscola, minuscola e carattere speciale) - FTE 0,5
2) Implementare sistemi di autenticazione MFA (garantiscono la protezione da attacchi bruteforce, da impersonificazione etc.) - FTE 2 (2days)
3) Impostare una scadenza nelle password per tutte le utenze (eventualmente implementare sistemi di Single Sign On che permettono la corretta gestione lato utente) - FTE 0,5
4) Utilizzare credenziali amministrative con username diversi da quelli di default (e.g. non usare utenze come admin, administrator etc. soprattutto su servizi esposti) - FTE 0,5

Bug nel codice
1)Gestire in modo più opportuno le verifiche sulla sessione e sui token per inibire la loro manipolazione tramite script - FTE 2 (3days)
2)Verificare che i reindirizzamenti tra i context/path e l'uso dei cookie di sessione non permettano di "bypassare" la login - FTE 2 (2days)
2)Implementare patch note su sistemi di attacco comuni come SQL Injection - FTE 1 (1day)

HTTP Methods e Headers

1) Abilitare i metodi HTTP necessari al singolo context, prestare attenzione ai metodi PUT, DELETE che permettono di operare sui contenuti - FTE 0,5
2) L'header restituito dalle pagine web dovrebbe mascherare la versione del web server che espone i servizi, altrimenti un eventuale attaccante potrebbe avere evidenza immediata delle vulnerabilità da sfruttare per la versione specifica - FTE 0,5

Robustezza Infrastruttura

1) Implementare una segmentazione a livelo di VLAN nel caso in cui si necessiti di implementare una rete Guest per gli ospiti - FTE 3 (5days)
2) Implementare l'uso di un web application firewall - WAF (per servizi web esposti) - FTE 1 (2days)
3) Implementare sistemi di backup con opportuna crittografia - FTE 2 (5days)
4) Implementare la ridondanza sui dispositivi critici per ridurre i tempi di inattività - FTE 3 (10days)
5) Implementare un piano DR (disaster Recovery) in caso di calamità naturale e/o simili (i sistemi cloud aprono a scenari Hybrid che aiutano a ridurre i costi in tal senso) - FTE 10 (20days)