Request for Information (RFI)

Vulnerability management

Sadržaj

1 Uvod

1.1 Ciljevi

Cilj ovog dokumenta je prikupljanje informacija za budući razvoj sistema upravljanja ranjivostima (eng. Vulnerability Management) BH Telecom-a za period 2024.-2026. godine, radi potencijalne nabavke platforme za testiranje ranjivosti.. Obzirom da BH Telecom u svojoj infrastrukturi ima 1000+ mašina na serverskoj infrastrukturi, na kojima su deploy-ane aplikacije za interne potrebe, kao i aplikacije koje su otvorene na Internetu, BH Telecom smatra jako važnim proces upravljanja ranjivostima. Također, obzirom da veliki broj uposlenika koji su geografski raspoređeni po čitavoj BiH, jako je bitno pratiti ranjivosti na radnim stanicama koje koriste uposlenici. Pored toga, BH Telecom posjeduje i više različitih kontejnerskih platformi na kojima su servisi kako za internu tako i za eksternu upotrebu te je obzirom na sigurnosne izazove koje nose ovakve platforme, potrebno vršiti adekvatno upravljanje ranjivostima.

1.2 Ciljana publika

Ovaj dokument je namijenjen kompanijama koje su vendori ili integratori rješenja za upravljanje ranjivostima. Rješenja koja nisu implementirana u okruženjima sa minimalno 500 asset-a u Evropi ili Sjevernoj Americi neće biti uzeta u razmatranje.

2 Opis okruženja

BH Telecom u svom okruženju posjeduje veliki broj asset-a koji su izloženi raznim sigurnosnim rizicima. Obzirom na veličinu kompanije, pošto imamo 3000+ uposlenih, koji su geografski raspoređeni po čitavoj BiH, u kompaniji se koriste raznorazni tipovi radnih stanica za različitm operativnim sistemima različitih verzija, Windows, Linux i Mac OS. Pored toga, obzirom da uposlenici jako često imaju potrebu da pristupaju resursima kompanije putem udaljenog pristupa, tj. VPN-a, koristi se i veliki broj radnih stanica za ove potrebe, a koje su pod kontrolom BH Telecom-a. Nerijetko se koriste i mobilni uređaji za pristup kolaborativnim alatima kao što je email, Microsoft Teams i slično. Obzirom na brojnost i raznolikost klijentskih urađaja koji se koriste od strane uposlenika, jako je zahtjevno odgovoriti na sve sigurnosne izazove koji ovi uređaji nose.

U dijelu serverske infrastrukture, BH Telecom posjeduje dva site-a, primarni i DR, na kojima je instaliran VMWare vSphere kao virtualizacijski sloj. Na ovoj infrastrukturi postoji 1000+ virtuelnih mašine koje se koriste za razne servise za interne potrebe BH Telecom. Pojedini servisi se koriste samo interno, tj. pristupaju im uposlenici BH Telecom, dok je određeni broj servisa otvoren na Internet (razne web aplikacije). Na ovakom velikom broju servera se koriste različite tehnologije u smislu web servera, programskih jezika, baza podataka i slično i jako je izazovno pratiti nove ranjivosti na svim serverima i aplikacijama. Pored ovoga, BH Telecom u svojoj infrastrukturi posjeduje i više različitih kontejnerskih platformi kao što je Openshift i Kubernetes. Zbog specifičnosti kontejnerskih aplikacija i mikroservisne arhitekture, jako je izazovno odgovoriti na sigurnosne zahtjeve. Trenutno rješenje koje se koristi je Qualys VMDR.

3 Zahtjevi

Platforma za upravljanje ranjivostima mora imati sljedeće karakteristike:

- Skeniranje asseta koji su javno dostupni na internetu u smislu skeniranja otvorenih portova i skeniranja ranjivosti korištenjem eksternih skenera sa Interneta.
- Skeniranje internih aseta u smislu skeniranja otvorenih portova i skenitanja ranjivosti korištenjem internih skenera.
- Mogućnost instalacije internog skenera na VMWare vSphere okruženju.
- Konfigurisanje različitih profila za skeniranje sa ograničavanjem broja portova, selekcijom određenih ranjivosti ili grupa ranjivosti.
- Skeniraniranje bez prethodne autentikacije na servis i skeniranje sa prethodnom autentikacijom na servis: SSH, Windows NTLM, SNMP, VMWare, HTTP Basic, MySQL, i slično.
- Mogućnost definisanja rasporeda skeniranja – dnevno, sedmično, mjesečno i sl.
- Klasifikacija ranjivosti po ozbiljnosti (severity).
- Mogućnost konfiguracije prioretizacije ranjivosti radi detekcije ranjivosti na kritičnim assetima
- Kreiranje izvještaja za ranjivosti.
- Mogućnost otvaranje ticketa za rješavanje ranjivosti i dodjeljivanjem ticketa odgovornoj osobi
- Grupisanje ranjivosti po assetima.
- Agent za razne verzije Windows OS-a, Linux-a, MacOS-a koji se može koristiti za identifikaciju ranjivosti na assetima.
- Skeniranje ranjivosti web aplikacija kao što je injection, XSS i slično, sa akcentom na OWASP Top 10 ranjivosti.
- Skeniranje ranjivosti kontejnerskih platformi kao što je Openshift i Kubernetes u smislu skeniranja ranjivosti korištenih image-a kao i skeniranje ranjivosti produkcionih kontejnera.
- Podrška za container runtime security.
- Mogućnost integracije sa SIEM alatima kao što je IBM QRadar.