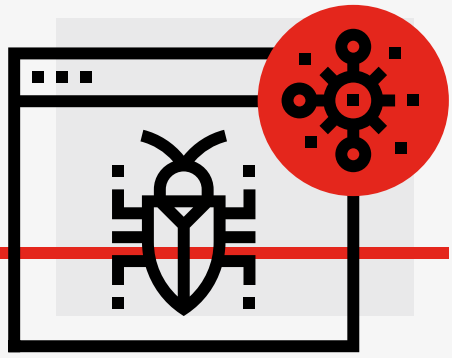
Skenovanie a správa ZRANITEĽNOSTÍ



Skenovanie zraniteľností (Vulnerability Scanning) a správa zraniteľností (Vulnerability Management) umožňuje lepšie riadenie bezpečnostných rizík a chráni vaše podnikanie alebo organizáciu. Mal by byť kľúčovou zodpovednosťou každého bezpečnostného IT tímu, prípadne poskytovateľa bezpečnostných služieb. Prináša a umožňuje najmä:

- **identifikáciu a zníženie bezpečnostných rizík**
- **automatizáciu správy zraniteľností**
- **doplnenie uceleného prehľadu o stave bezpečnosti IT infraštruktúry**
- **zabezpečenie súladu so štandardmi, legislatívou a internými politikami**
- **rozšírenie pohľadu na riadenie rizík integráciou s nástrojmi tretích strán**
- **ochranu dobrého mena organizácie**

Skenovanie zraniteľností zahŕňa hodnotenie, odporúčaný spôsob nápravy a vytváranie správ/reportov o všetkých objavených zraniteľnostiach, ktoré existujú v systémoch a v infraštruktúre organizácie. Jeden z najúčinnejších spôsobov, ako uvedené dosiahnuť, je prostredníctvom automatizovaného systému na sken známych zraniteľností.

Skener zraniteľností je aplikácia, ktorá identifikuje a vytvára inventár všetkých aktív (vrátane serverov, počítačov, virtuálnych počítačov, kontajnerov, brán/firewall-ov, sieťových prvkov a tlačiarní) pripojených k sieti. Pre každé zariadenie, ktoré identifikuje sa tiež pokúsi identifikovať operačný systém, ktorý sa na ňom prevádzkuje. V mnohých prípadoch je skener schopný zistiť aj nainštalovaný aplikačný softvér spolu s ďalšími atribútmi, ako sú otvorené porty a používateľské účty.

Pre koho je sken zraniteľností určený?

Organizáciám s akoukoľvek veľkosťou IT infraštruktúry.

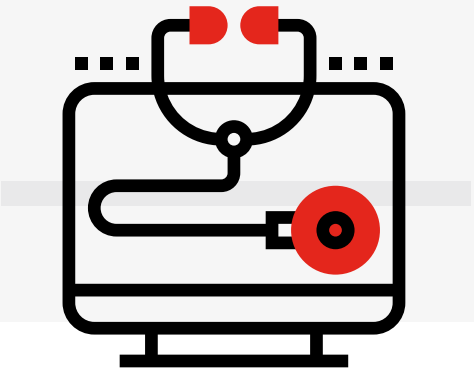
Aj prísne zabezpečené siete a systémy môžu obsahovať zraniteľnosti, ktoré v čase implementácie neboli publikované/známe. Práve mylný dojem „dokonalého“ zabezpečenia infraštruktúry spôsobuje v konečnom dôsledku nemalé finančné straty a častokrát aj poškodenie dobrého mena organizácie. Pravidelným skenovaním IT infraštruktúry sa dá zabrániť ako finančným stratám, tak aj poškodeniu dobrého mena organizácie.

Tempest
IT makes sense

Prečo je potrebné riešiť skenovanie a následnú správu zraniteľností?

Skenovanie a správa zraniteľností je dôležitou súčasťou pre správne fungovanie bezpečnostného IT tímu, nakoľko umožňuje lepšie riadenie rizík, respektíve im predchádza. Skener identifikuje systémy a časti IT infraštruktúry, na ktoré aplikuje sadu testov. Výsledky z týchto testov odhalia bezpečnostné zraniteľnosti. Takéto informácie je potrebné využiť vo svoj prospech a teda snažiť sa odstrániť nájdené bezpečnostné zraniteľnosti skôr, ako by mohli byť zneužité potenciálnym útočníkom. Odstraňovanie zraniteľností prebieha vo všeobecnosti v štyroch krokoch:

1. **identifikácia zraniteľností**
2. **vyhodnotenie rizikovosti zraniteľností (tzv. scoring)**
3. **odstránenie zraniteľnosti**
4. **reportovanie nájdených a odstránených zraniteľností**

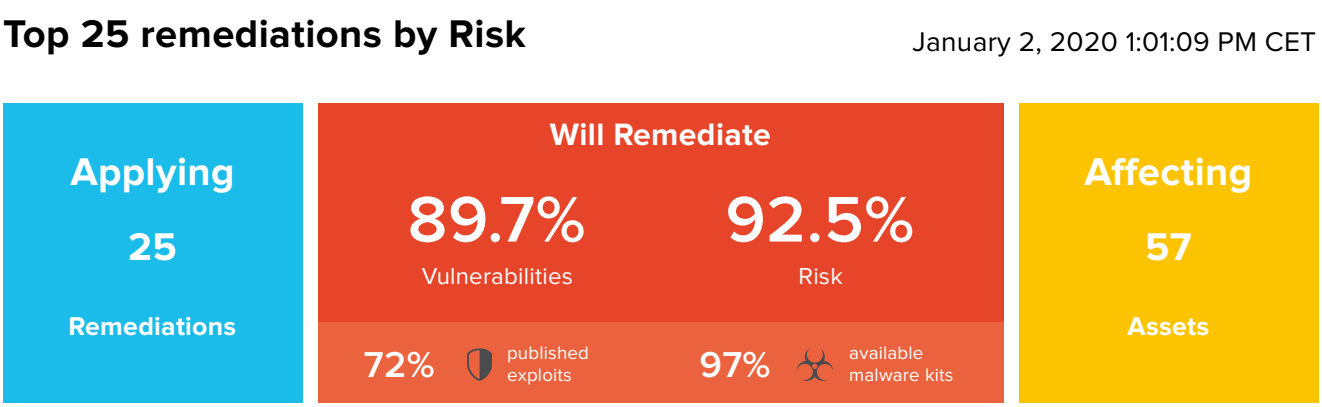


1. Identifikácia – Identifikácia zraniteľností pomocou správne implementovaného a nastaveného automatizovaného nástroja na sken známych zraniteľností. Dôležitou podmienkou pre skener je jeho dôsledná integrácia do IT infraštruktúry organizácie.

2. Vyhodnotenie rizikovosti danej zraniteľnosti – Aby nebol bezpečnostný tím zahltený množstvom informácií a vedel sa rozhodnúť, ktoré zraniteľnosti riešiť prioritne, je potrebné daným zisteniam priradiť závažnosť. Súčasťou výstupov skenu zraniteľností je aj takzvaný skóring danej zraniteľnosti, na základe ktorého vie bezpečnostný tím nastaviť priority ich eliminácie.

3. Odstránenie zraniteľnosti – Ideálnym riešením odstránenia nájdenej zraniteľnosti je aplikovanie opravného patchu alebo updatu. Takéto riešenie však nie je vždy možné a vtedy je potrebné aplikovať iný prístup k zmierneniu vzniknutého rizika. Takéto odstraňovanie zraniteľností sa dá manuálne len veľmi ťažko riadiť a kontrolovať. Z tohto dôvodu si nástroj pamätá predošlé nálezy, eviduje stav ich riešenia a prehodnocuje celkovú zraniteľnosť infraštruktúry alebo systému.

4. Reportovanie nájdených a odstránených zraniteľností – Reportovanie zraniteľností je dôležitou súčasťou a ukončením jedného cyklu procesu odstraňovania zraniteľností. Reporty graficky upozorňujú na aktuálny stav infraštruktúry aj osoby mimo bezpečnostný tím. Príklad takéhoto reportu je uvedený nižšie.



Obr.: Nájdené zraniteľnosti, príklad.

Súlad s bezpečnostnými štandardmi a legislatívou

Zabezpečenie pravidelného skenu zraniteľností je nevyhnutné na zabezpečenie súladu organizácií s požiadavkami najmä nasledovných bezpečnostných štandardov a legislatívy:

- zabezpečenie súladu s požiadavkami **ISO/IEC 27001** a **ISO/IEC 20000-1**
- zabezpečenie ochrany infraštruktúry podporujúcej prevádzku základných služieb v zmysle **zákona** č. 69/2019 Z.z. **o kybernetickej bezpečnosti** a s nadväzujúcimi vyhláškami
- zabezpečenie ochrany osobných údajov spracúvaných v informačných systémoch v zmysle nariadenia **GDPR**, resp. **zákona** č. 18/2018 Z.z. **o ochrane osobných údajov**
- zabezpečenie ochrany informačných systémov a technológií verejnej správy v zmysle požiadaviek zákona č. 95/2019 Z.z. o informačných technológiách vo verejnej správe
- zabezpečenie ochrany kritickej infraštruktúry v zmysle požiadaviek **zákona** č. 45/2011 Z.z. **o kritickej infraštruktúre**

O nástrojoch na sken a správu zraniteľností

Vďaka bohatým skúsenostiam vie spoločnosť TEMPEST zabezpečiť skenovanie prostredníctvom nástrojov od spoločnosti Rapid7 (InsightVM, Nexpose). Tieto nástroje umožňujú live manažment zraniteľností a analýzu koncových bodov za účelom sledovania zraniteľností organizácie v reálnom čase. Nástroje dokážu nájsť zraniteľnosti, informácie o nich efektívne spracovať a prípadne ich aj exportovať do iných nástrojov ako je napr. SIEM. Tieto nástroje je možné integrovať aj s cloud službami, virtuálnou infraštruktúrou, ako aj s kontajnermi.

Možnosti realizácie skenu zraniteľností

1. **Vykonanie jednorazového skenu**
2. **Vykonávanie pravidelného skenu**
3. **Implementácia nástrojov na skenovanie a správu zraniteľností do infraštruktúry**

Jednorazový scan

TEMPEST vykoná sken na známe zraniteľnosti pomocou prenosného zariadenia, na ktorom je nainštalovaný a predpripravený automatizovaný nástroj na sken zraniteľností. Host vykonávajúci sken musí byť umiestnený do skenovanej infraštruktúry a musí mať sieťovú viditeľnosť na všetky zariadenia, ktoré sú predmetom kontroly. Takýto sken môže byť vykonaný na podnet zákazníka kedykoľvek a zákazník tak získa komplexný obraz o zraniteľnostiach nachádzajúcich sa v infraštruktúre v čase skenovania. Po vykonaní skenu je zákazníkovi odovzdaná správa a reporty z tejto akcie. Správa obsahuje aj odporúčania na odstránenie nájdených zraniteľností, ale aj odporúčania na predchádzanie zraniteľnostiam do budúcna.

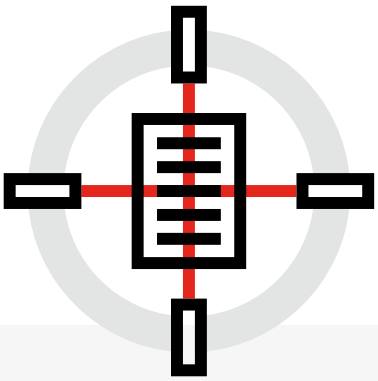
Pravidelný scan

TEMPEST ponúka službu výkonu pravidelného skenovania zraniteľností. Jedná sa o podobnú aktivitu ako pri jednorazovom skene, s tým rozdielom, že sken je vykonávaný vo vopred definovanom časovom intervale. Takéto pravidelné skenovanie dovoľuje zobraziť tendenciu vývoja a odstraňovania zraniteľností v čase, čo má za následok zvýšenú bezpečnosť infraštruktúry a systémov. Práve sledovanie zraniteľností v čase vie lepšie určiť slabé miesta v infraštruktúre, a teda zabezpečiť lepšie smerovanie bezpečnostného tímu. Zákazník mimo správy a reportu získa aj „pohľad“ do minulosti a na vývoj zabezpečenia svojej infraštruktúry.

Implementácia nástroja na sken a správu zraniteľností do infraštruktúry

Za najlepšiu možnosť sledovania známych zraniteľností v infraštruktúre považujeme nasadenie skeneru zraniteľností priamo do infraštruktúry organizácie. Takto integrovaný skener môže vykonávať testy podľa vopred definovaných časových intervalov, ale dovoľuje aj spúšťať skeny podľa aktuálnej potreby iba na vybrané aktíva. Skener, ktorý je stálou súčasťou infraštruktúry dovoľuje zbierať dáta o zraniteľnostiach najpresnejšie, čo zabezpečuje lepší skóring pre nájdené zraniteľnosti a systémy, na ktorých boli tieto zraniteľnosti objavené.

Takto integrovaný skener dovoľuje skenovanie zariadení nielen vo vybranom čase, ale skenovanie zariadenia sa môže vykonávať hneď po prihlásení sa do siete organizácie, prípadne po objavení nového zariadenia. Takýmto skenovaním je vylúčená možnosť vynechania skenu zariadení, ktoré boli v čase pravidelného skenu nedostupné alebo vypnuté. Taktiež umožňuje implementácia tohto nástroja lepšie manažovanie a kontrolu odstraňovania zraniteľností. Ak je zraniteľnosť administrátorom označená za odstránenú, skener vykoná jednorazovo rýchly test tejto odstránenej zraniteľnosti a preverí, či bola skutočne odstránená, resp. či nepribudla iná zraniteľnosť. Zákazník má teda lepší prehľad o zraniteľnostiach nachádzajúcich sa v infraštruktúre a má lepšie možnosti manažovania ich odstraňovania.



Prečo TEMPEST?

Spoločnosť TEMPEST realizovala už viacero skenovaní zraniteľností infraštruktúry zákazníkov a má za sebou viaceré implementácie nástrojov na skenovanie zraniteľností. Medzi pravidelných zákazníkov našej spoločnosti patria inštitúcie z bankového sektora, výroby ale aj verejnej správy.

Spoločnosť TEMPEST má taktiež dlhoročné skúsenosti s vykonávaním penetračných testov, ktoré na základe nástrojov a postupov preveria bezpečnosť infraštruktúry organizácie, informačných systémov alebo web aplikácií. Tieto činnosti sú samozrejme vykonávané v súlade so základnými pravidlami etického hackingu.

V spoločnosti disponujeme špecialistami s dlhoročnými skúsenosťami s vykonávaním skenov zraniteľností a penetračných testov disponujúcimi certifikátmi ako sú CEH-Certified Ethical Hacker, CISSP-Certified Information Systems Security Professional, CRISC-Certified Risk and Information Systems Control a ďalšie.

Viac o spoločnosti TEMPEST na www.tempest.sk.

TEMPEST a.s.
EBC, Krasovského 14
851 01 Bratislava 5
Slovenská republika

Tel.: +421 2 502 67 111
Fax: +421 2 502 67 129
E-mail: info@tempest.sk
Web: www.tempest.sk

Tempest
IT makes sense