IngramMicroCyberSecurity

Vulnerability Assessment

Tjänstebeskrivning

Version: 3.0

Innehållet

1. Inledning

Säkerhetsrisker utvecklas ständigt allt eftersom angriparna (hackarna) utvecklas och hittar nya systemsvagheter för att få tillgång till information i organisationers system. *Vulnerability Assessment* (VA) är processen för att hitta, identifiera, klassificera och rapportera säkerhetsluckor och brister. I takt med att företag fortsätter utöka sina IT tjänster och nätverk ökar också konsekvenserna av att ha säkerhetsluckor i systemen. Därför måste organisationer aktivt bedöma förekomsten av säkerhetsluckor i nätverket och vidta åtgärder för att identifierade och minimera konsekvensverkan av dessa.

2. Tjänstens syfte

Syftet med tjänsten *Vulnerability Assessment* är följande:

- Identifiera sårbarheter och säkerhetsrisker som illvillig användare eller part kan nyttja för att utsätta en organisations IT-resurser för haverier eller funktionalitetsförluster. IT-resurserna inkluderar nätverksenheter, servrar, skrivare, applikationer och klienter.
- Klassificera upptäckta sårbarheter efter risknivåer och allvarlighetsgrad.
- Förbättra säkerheten i organisationen genom att proaktivt identifiera säkerhetsbrister och felaktiga konfigurationer som finns i IT-resurserna samt tillhandahålla nödvändiga åtgärder.

3. Tjänstens omfattning

Tjänsten *Vulnerability Assessment* omfattar alla IT-resurser som är anslutna till organisationens nätverk. Tjänsten visualisera en organisations aktuella säkerhetsstatus och effektiviteten av motåtgärder som har implementerats för att skydda mot cyberhot. *Vulnerability Assessmentar* utförs i två varianter:

- **External Vulnerability Assessment** (Bedömning av externa sårbarheter)**:** Utförs på distans av vårt SOC-team. Målet med testet är att identifiera och klassificera svagheterna i en organisations IT-resurser som är publicerade mot Internet som webbapplikationer, webbservrar, nätverksutrustning, VPN och e-postservrar. Testet hjälper säkerhetsansvariga i en organisation att veta vilka externa IT-resurser som behöver omkonfiguration, uppdateringar eller åtgärdas på annat sätt.
- **Internal Vulnerability Assessment** (Bedömning av interna sårbarheter): Utförs inifrån organisationens interna nätverk, vanligtvis för att identifiera och klassificera hot och brister i det interna nätverket. Detta hjälper också en organisation att fastställa dess överensstämmelse med globala eller lokala policyer, standarder och förfaranden när det gäller informationssäkerhet, dataskydd och segmentering av nätverk.

4. Tillvägagångssätt

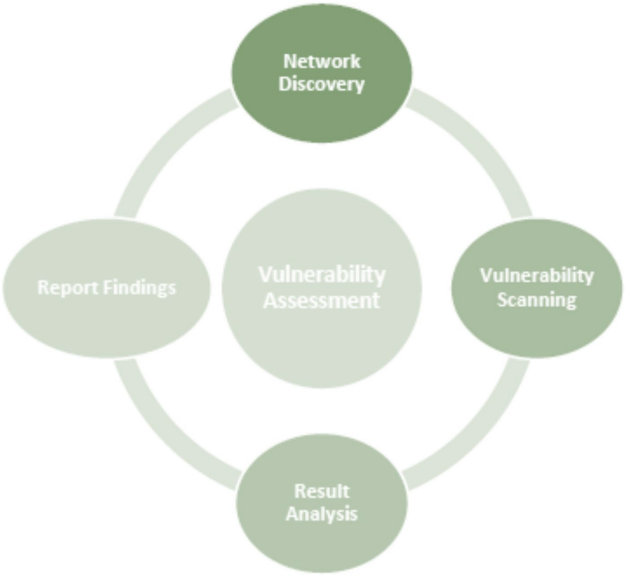
Vulnerability Assessment utförs vanligtvis enligt följande steg:

1. **Network Discovery** (Nätverksidentifiering)**:** identifiera nätverkets IT-resurser och bekräfta att dessa tillgångars giltighet i organisationen.

2. **Vulnerability Scanning** (Sårbarhets Skanning)**:** Genomsökning och identifiering av IT-resursers kända säkerhetsbrister.

3. **Result Analysis** (Resultatanalys)**:** Genomgång av identifierade sårbarheter och eliminering av testresultat som kan felaktigt indikerar vissa attribut.

4. **Report Finding** (Konstaterande)**:** rapportera identifierade sårbarheter inklusive effektklassificering och rekommenderade åtgärder för att minimera konsekvensverkan.



Ingram Micro kommer att använda en kombination av automatiserade och manuella metoder för att identifiera olika sårbarheter och eliminera felaktiga resultat.

5. Förutsättningar

För att säkerställa ett lyckat och smidigt genomförande av tjänsten *Vulnerability Assessment* måste vissa förutsättningar vara på plats enligt följande:

- **External Vulnerability Assessment** (Bedömning av externa sårbarheter)**:** IP-adresser för de resurser som skall inkluderas i testet.
- **Internal Vulnerability Assessment** (Bedömning av interna sårbarheter)**:** En virtuell maskin (VM) för att installera våra säkerhets verktyg som kommer att användas för att utföra skanningen och för att samla in data. Den virtuella datorn ska ha följande specifikation:
    - **Maskinvarukrav:** 4 GB RAM, 100 GB lagringsutrymme och 2 Core-processor.
    - **Nätverksåtkomst:** VMen bör placeras i ett VLAN som har access till alla nätverkssegment och VLAN som ska vara med i testet. Dessutom bör den virtuella datorn vara tillgänglig från Internet så att Ingram Micros SOC-team kan komma åt via VPN eller fjärrskrivbord för att underlätta fjärrhantering och utförande av tjänsten.
    - **Programvara:** En image kommer att distribueras och skall installeras på ovan nämnda VM. Så snart imagen har installerats kommer den att be om aktiveringskod som kommer att tillhandahållas av Ingram Micros SOC-team.

6. Rapport

När testet har slutförts skickas en detaljerad rapport till kunden som inkluderar följande:

- **Executive Summary** (Sammanfattning)**:** Sammanfattning av testresultatet med en bedömning samt en kortfattad redogörelse av hotbilden som organisationen utsätts för ur ett affärsperspektiv.
- **Findings** (Resultaten)**:** En detaljerad teknisk beskrivning av testresultatet med bevisningar.
- **Conclusions & Recommendations** (Slutsats & rekommendationer)**:** Det här avsnittet innehåller en sammanfattning av de problem som hittats under testet med eventuella rekommendationer för åtgärder.

7. Leveransvillkor

Tjänsten Vulnerability Assessment på ca 100 IT-resurser kan levereras inom 10 arbetsdagar efter angivet startdatum.
Testet påbörjas vid, av återförsäljare angivet, datum.

8. Antaganden

- Vulnerability Assessment kommer att utföras från Ingram Micro i Tyskland.
- Kunden kommer att tillhandahålla alla nödvändig information, i detta fall IP-adressintervall, VM och tillgång till VM för intern Vulnerability Assessment. Men för extern Vulnerability Assessment behövs enbart de publika IP-adresserna.
- Kunden är ansvarig för att anordna nödvändiga möten med relevanta intressenter för att framgångsrikt utföra tjänsten.
- Kunden är ansvarig för att ge feedback och/eller signera slutleveransen inom fem arbetsdagar efter att rapporten gjorts tillgänglig av Ingram Micro.
- Kunden ansvarar för att genomföra nödvändiga åtgärderna som rekommenderas i testrapporten.
- Ingram Micros SOC-team kommer att tillhandahålla dokumentation med nödvändiga åtgärdsförslag för eventuella funna brister.
- Ingram Micros SOC-team ansvarar inte för att fastställa/åtgärda någon av funna sårbarheterna utan endast för att tillhandahålla dokumentation för hur eventuella problem kommer kunna åtgärdas.

Kontakta oss

Har du frågor om vår tjänst **Vulnerability Assessment** är du välkommen att kontakta oss på:

csec.nordics@ingrammicro.com eller +46-708-234740

Shawn Akrawi
Business Development Manager

Andreas Pantzar
Sales Specialist

9. Bilaga – A – vanliga frågor

Vad innebär Sårbarhetsbedömning (Vulnerability Assessment)?

Sårbarhetsbedömning är en nulägesutvärdering av IT-säkerhetsmekanismerna i kundens IT-miljö/nätverk. Bedömningen syftar till att avslöja befintliga brister som bör uppmärksammas och utredas djupare. Metoden är utmärkt för att identifiera brister, men inkluderar inte validering av befintliga brister eller försök att utnyttja bristerna.

Kan en skanning av sårbarheterna i ett nätverk skapa driftstörningar eller ha annan påverkan?

Automatiserade tester eller scanning har ingen driftpåverkan eftersom det är en sk icke-invasiv skanning. Skanningen kommer endast att söka efter nätverkets eller webbservrarnas sårbarheter, men kommer inte att kontrollera säkerhetsfrågor som t. ex. parameter manipulations test, DOS-tester, Buffer Overflow tester etc.

Hur utförs extern och intern Vulnerability Assessment?

Extern sårbarhetsskanning kan utföras från Internet. För intern skanning kommer en virtuell maskin att behövas i kundens interna nätverk. Den virtuella maskinen kommer inte att påverka nätverket negativt, utan kommer endast att kommunicera med externa scanning verktyg för att kontrollera sårbarhetssignaturer.

Hur rankar Ingram Micros SOC-team sårbarheterna i kategorierna Kritiskt/Hög/Medel/Låg?

Ingram Micros SOC-team använder följande metod för kategorisering/ranking/värdering/prioritering av sårbarheter:

- Allvarlighetsgrad som rapporterats av testverktyget
- BII (Business Impact index) för IT-resursen
- Publik, interna eler DMZ placerade resurs
- Exploaterande eller icke-exploaterande sårbarhet
- Finns det fix/patch/åtgärd tillgänglig för åtgärda sårbarheten

10. Bilaga - B – Verktyg

Ingram Micro använder en blandning av automatiserade och manuella test metoder för att upptäcka eventuella sårbarheter i ett nätverk. Vi använder oss av väl kända gratis samt kommersiella säkerhets verktyg. Vi använder bland annat följande applikationerna:

- **Maltego:** Ett verktyg som används vid penetrationstester samt i Public Discovery rapporter.
- **NMAP:** Ett nätverksskanner applikation som används för att mappa och lista nätverks enheter som är en del i ett penetrationstest.
- **Nessus:** En sårbarhetsskanner som används för att upptäcka sårbarheter och Malware som angripare kan använda för att ta sig in i ett nätverk. Nessus används som en del i sårbarhetsrapporter samt penetrationstester.
- **Qualys:** En nätverks och sårbarhetsskanner som används i Webbapplikationstester och vid penetrationstester.
- **Kali Linux distribution:** Ett operativsystem med hundratals verktyg som kan användas för alla typer av tester.
- **Burp Suit:** En webbaserad Proxy som används vid webbapplikationstester och vid webbpenetrationstester.
- **BeEF:** Används för webbtester som exploateringsverktyg.
- **OWASP proxy:** En lokal Proxy som används vid webb och mobilapplikationstester.
- **Metasploit:** Ett ramverk för penetrationstest som används för exploatering och i bedömning av penetrationstester efter exploatering.