factsheet

Uw organisatie, door de ogen van een kwaadwillende

Als organisatie wilt u natuurlijk goed zichtbaar zijn voor klanten en potentiële werknemers. Helaas proberen ook kwaadwillenden op het internet uw organisatie zo goed mogelijk te leren kennen en gaan ze op zoek naar mogelijke ingangen om uw data buit te maken en uw organisatie verder binnen te dringen [1-3]. Deze factsheet neemt u mee in wat u zelf kunt ontdekken over uw organisatie, kijkend door de ogen van een kwaadwillende.

Vacatures en profielen van (ex-) medewerkers

Wat vertellen uw openstaande en historische vacatures over uw IT-inrichting? Heeft u de vacaturepagina van uw website wel eens bekeken via het internetarchief? Wat vertellen uw (ex-) medewerkers op LinkedIn over welke IT-applicaties ze vaardig in zijn? Hoe meer een kwaadwillende zicht heeft op hoe de IT bij uw organisatie is ingericht, hoe gerichter de kwaadwillende kan zoeken naar mogelijke kwetsbaarheden in IT-producten waar u afhankelijk van bent. Welke medewerkers en online beschreven functieprofielen, met contactgegevens, zijn bijvoorbeeld erg uitnodigend voor kwaadwillenden om een phishingmail naartoe te sturen?

Actiepunten:

- Controleer: uw eigen website, https://www.linkedin.com/ en https://archive.org/web/
- **Voorbeeld:** https://web.archive.org/web/20210715000000*/ https://z-cert.nl/werken-bij-z-cert/

Nieuwsberichten door uzelf en van uw leveranciers

Wat vertellen nieuwsberichten op uw eigen website en nieuwsberichten op de website van uw leveranciers over de inrichting van uw IT? Zijn er recente berichten over migraties in uw IT-landschap of zijn er berichten over aanbestedingen met daarin specifieke details over uw organisatie? Met welke leveranciers of andere organisaties bent u recent een samenwerking aangegaan. Dit levert mooie en actuele input op voor gerichte phishingberichten.

Actiepunten:

- Controleer: uw eigen website, de websites van uw leveranciers en https://archive.org/web/
- **Voorbeeld:** https://z-cert.nl/z-cert-geeft-startschot-voor-levering-soc-diensten/

Certificaten van uw internetdomeinen

Het internet maakt gebruik van certificaten om te controleren of gegevens veilig worden verzonden. Wat vertellen de internetcertificaten van uw domeinnaam over de IT-inrichting van uw organisatie? Maakt u wel gebruik van twee afzonderlijke Certificate Authorities (CAs), eentje voor uw interne domeinen en eentje voor externe domeinen? In hoeverre geven deze certificaten een kwaadwillende inzicht in uw interne infrastructuur?

Actiepunten:

- Controleer: crt.sh/
- **Voorbeeld:** https://crt.sh/?q=z-cert.nl

Online bestanden bij clouddiensten

Welke bestanden van uw bedrijf zijn via clouddiensten direct toegankelijk via het internet? En staan in deze bestanden toevallig sensitieve gegevens, zoals wachtwoorden op Github, of andere bedrijfsinterne informatie die een kwaadwillende kan inzetten om zich voor te doen als een interne medewerker?

Actiepunten:

- Controleer Google of een andere zoekmachine, zoals DuckDuckGo, op gevoelige bestanden. Voer b.v. bij Google search "filetype:docx", "filetype:pdf" of "filetype:csv" in, gecombineerd met de domeinnaam van uw organisatie.
- **Voorbeeld:** https://duckduckgo.com/?va=c&t=hl&q=filetype%3Apdf+z-cert&ia=web
- Controleer publiektoegankelijke cloudbuckets van b.v. Amazon of Microsoft op gevoelige bestanden. Dit kan door gebruik te maken van diensten als https://buckets.grayhatwarfare.com/files.
- Controleer of https://github.com geen gevoelige informatie bevat van uw organisatie, zoals wachtwoorden of api-keys.

Aan het internet verbonden apparaten

Wat vertellen internet (kwetsbaarheden) scanners over uw organisatie? Heeft u zicht op welke (Internet of Things) apparaten, servers en routers van uw organisatie aan het internet verbonden zijn? Internet (kwetsbaarheden) scanners, zoals Shodan en Censys scannen dagelijks het hele internet af naar alles wat verbonden en direct toegankelijk is.

Actiepunten:

- Controleer: https://search.censys.io/, https://www.shodan.io/
- **Voorbeeld:** https://www.shodan.io/domain/z-cert.nl

Open Source Intellingence

Deze factsheet bespreekt bekende technieken voor het onderzoeken van een organisatie met behulp van open bronnen en publiektoegankelijke informatie, Open Source Intelligence (OSINT). Door bewust te zijn over wat er over uw organisatie op het internet vindbaar is, kunt u keuzes maken over wat u wel en niet wilt delen met mogelijke kwaadwillenden.

COMPUTER EMERGENCY
RESPONSE TEAM
VOOR DE ZORG

Bronnen

[1] https://www.bnr.nl/nieuws/technologie/10541786/tientallen-open-servers-bij-nederlandse-bedrijven-gegevens-op-straat
[2] https://z-cert.nl/eerste-red-teaming-oefening-antoni-van-leeuwenhoek-ziekenhuis-en-z-cert/
[3] DIFx Live, 2022, Wat is de digitale voetafdruk van jouw bedrijf? https://www.youtube.com/watch?v=8ULODJJWcKM