

Live Check: Was über Ihr Unternehmen im Darknet
und Internet kursiert



Was ist OSINT?

Erkenntnisgewinn aus Quellen die Jedermann zur Verfügung stehen.

Jedermann = Jeder ohne besondere Fähigkeiten

Quellen müssen nicht kostenlos sein

OSINT beschränkt sich nicht auf das Internet



Ablauf von OSINT

Informationen sammeln

Daten extrahieren

Aus Daten Erkenntnisse gewinnen



OSINT Quellen

Suchmaschinen

Soziale Netzwerke (LinkedIn, Instagram, WhatsApp)

Bewertungsportale (kununu, TrustPilot,...)

Parkbänke

Mülltonnen



Arten der Aufklärung

Direkte Aufklärung

- Gebäude beobachten
- Anrufen und nach Informationen fragen
- Gebäude betreten

Digitale Aufklärung

- Was gibt die Webseite an Informationen?
 - Haben Mitarbeiter Instagram Accounts?
 - Sind Informationen auf Fotos verwertbar?
 - Was sagt die KI?
-



Daten und Erkenntnisse

Am Beispiel von Spiegelmining (David Kriesel 33c3)

Informationen: Neue Artikel auf Spiegel Online beobachtet
über 2 Jahre.

Datenextraktion: Wann kamen neue Artikel? Von wem?
Und aus welchem Ressort



Daten und Erkenntnisse

Erkenntnisse:

- Am Montag sind die Redakteure am motiviertesten
(lange Artikel)
 - Die Kulturredaktion schläft am längsten (erste Artikel erst um 9 Uhr)
 - Die Redaktionen bleiben hauptsächlich unter sich.
(Zusammenhang der gleichzeitig veröffentlichten Artikel)
-



Einsatz der Erkenntnisse

- Weiterverkauf im Falle von Industriespionage
- Pentesting / Redteaming
- Spear Phishing



theHarvester

- automatisches OSINT im digitalen Raum
- fragt
 - Suchmaschinen
 - Schwachstellendatenbanken
 - Domain Name Server
 - LinkedIn
 - Test auf anfällige Webserver
- ergibt ein gutes Lagebild über die digitale Infrastruktur



theHarvester

```
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml
*****
*
* theHarvester
*
* theHarvester 4.11.1
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****

[*] Target: secuworx.de

Read api-keys.yaml from /etc/theHarvester/api-keys.yaml
Failed to process bevigil search for word: 'secuworx.de'
Error Message:
[!] Missing API key for bevigil.
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml

[!] Missing API key for Bitbucket.
```

Werkzeuge Online

- haveibeenpwnd.com
 - Webseite zur Überprüfung von E-Mail-Adressen und Passwörtern
 - Regelmäßige Prüfung empfohlen
- ssllabs.com
 - Prüft öffentlich erreichbare Server auf SSL/TLS
 - 1x im Quartal kann z.B. bei ISO 27001 helfen
- mxtoolbox.com
 - Prüft Ihren Mailserver auf Funktion und Black Listing
 - u.a. SPF / DKIM / DMARC Tests



Resilience aufbauen

- Keine Fotos mit Firmenlogo
- Keine Fotos mit Firmenausweisen
- Social Media auf das Nötigste beschränken
- Keine unternehmensbezogenen Fotos auf Privataccounts
- Routinen brechen
- Namen externer Dienstleister erfassen und abfragen
- Transaktionen bestätigen (Zweiter Faktor)
- Sichtschutzfolien an den Fenstern
- Bildschirme nicht gegenüber von Fenstern aufstellen



Das Darknet

- Lediglich ein anderer Teil des Internets
- Wenn Sie sich nicht sicher sind: Gehen Sie nicht hin.
- Seien Sie vorsichtig.
- Kryptowährungen sind die Währung des Darknet.

