TÜV TRUST IT
TÜV AUSTRIA Group

Cyber Security

Open Source Intelligence (OSINT) – Ermittlungen im Internet

Die Abwehr von Cyber-Angriffen steht bei Unternehmen ganz oben auf der Agenda. Und das zu Recht, denn die Gefahr durch Cyber-Kriminalität ist aktueller denn je. Open Source Intelligence (OSINT) Analysen helfen Ihnen dabei eine klare Übersicht über die Angriffsfläche Ihres Unternehmens zu behalten.

Vorgehensweise

Unsere erfahrenen Security-Analysten identifizieren die öffentlich über das Internet erreichbaren Systeme Ihrer IT. Durch den Einsatz von spezialisierten Werkzeugen, APIs und fortgeschrittenen Untersuchungstechniken werden verschiedenste öffentlich verfügbare Informationen über Ihr Unternehmen (z.B. wie Hostadressen, Nameserver, MX Server, Zone Transfers, Scraping von E-Mail-Adressen usw.) aggregiert.

Die gewonnenen Informationen können im nächsten Schritt (optional zusätzliche Dienstleitung) genutzt werden, um Systeme einer tiefer gehenden Sicherheitsanalyse (Penetrationstest) zu unterziehen.

Handeln wie ein „tatsächlicher“ Angreifer

Unsere Analysten orientieren sich bei ihrer OSINT Analyse an der Vorgehensweise „tatsächlicher“ Angreifer, die nach allen verfügbaren Informationen über ihre Opfer recherchieren, bevor sie damit beginnen ein Unternehmen anzugreifen.

Vor der OSINT Analyse erhalten unsere Security-Analysten keinerlei Informationen über Ihr Unternehmen und Ihre interne Infrastruktur. Das Ziel der Analyse ist die Gewinnung von Informationen (Information Gathering) über die IT-Infrastruktur Ihres Unternehmens.

Die OSINT Analyse besteht aus vier Phasen: Abstimmung der Voraussetzungen (Szenarien, Umfang), Informationsbeschaffung, Auswertung und Erstellung des Berichts. In der ersten Phase wird mit dem Kunden abgestimmt, welche Szenarien und Umfang bei der OSINT Analyse durchgeführt werden.

Szenarien

Während der Open Source Analyse sollen insbesondere folgende Szenarien durchgeführt werden:

- Komplexe Suche der Informationen auf verschiedenen Suchwerkzeugen ohne Eindringversuche in die IT-Infrastruktur.

Phasen der OSINT-Analyse

Cyber Security

- Sammlung der Informationen auf sozialen Netzwerken (z.B. XING, LinkedIn, Facebook, Twitter, Instagram usw.)

Detaillierter Bericht

Alle gewonnenen Informationen werden in einem detaillierten Bericht zusammengefasst und auf Kundenwunsch in einer Telefonkonferenz oder Termins vor Ort erläutert und diskutiert. Der Abschlussbericht wird dem Auftraggeber elektronisch zur Verfügung gestellt. Hier können weitere Schritte diskutiert werden (z.B. ob die identifizierten Systeme in einer tiefer gehenden Sicherheitsanalyse (Penetrationstest) untersucht werden sollen).

Ihr Nutzen

- Übersicht über die Angriffsfläche Ihres Unternehmens
- Detaillierter Abschlussbericht
- Möglichkeit in dem nächsten Schritt die identifizierten Systeme in einer tiefer gehenden Sicherheitsanalyse (Penetrationstest) zu untersuchen
- Die Kompetenzen der TÜV TRUST IT zur Durchführung von Penetrationstests wurden durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit der Zertifizierung zum zertifizierten IT-Sicherheitsdienstleister bestätigt.

TÜV TRUST IT GmbH
Unternehmensgruppe TÜV AUSTRIA

Waltherstraße 49–51
D-51069 Köln
Tel.: +49 (0)221 969789 - 0
Fax: +49 (0)221 969789 -12

TÜV TRUST IT
TÜV AUSTRIA GmbH

Wienerbergstraße 11
Turm B, 2. Stock · A-1100 Wien
Tel.: +43 (0) 5 0454 - 1000
Fax: +43 (0) 5 0454 - 76245

info@tuv-austria.com
www.it-tuv.com