Das Darknet – Millionen Userdaten sind im Netz verfügbar

Es gibt ein dunkles Kellergeschoss unterhalb vom freien und nützlichen sowie für Jedermann unkompliziert zugänglichen Internet. Dort lassen sich nicht nur Drogen oder Waffen kaufen, wie am Beispiel des Amokschützen in München zu sehen war, sondern auch Auftragskiller bestellen. Dort floriert auch der illegale Handel mit Nutzerdaten.

Das „gewaltige Paralleluniversum des Darknet dient überwiegend dem illegalen Zweck", weiß der IT-Sicherheitsexperte Marcel Jordan, EDV-Sachverständiger und IT-Forensiker aus Sinntal-Altengronau. Hier sein Erfahrungsbericht mit dem „Dunklen Netz" und welche Lösungen er Unternehmen vorschlägt.

Google & Co. kennen nur einen Teil

Ich habe mir in den vergangenen Jahren bei meinen Auftraggebern aus der Privatwirtschaft, aber auch aus Behörden und Kommunen, einen etablierten Namen in Sachen IT-Sicherheit erarbeitet. Ich bin in der Szene bestens vernetzt – und doch gibt es Dinge, die auch ich nicht erwartet hätte.

Vor kurzem habe ich im Kundenauftrag an einer bundesweiten Awareness-Schulung für IT-Verantwortliche teilgenommen. Sie entsprach dem neuen IT-Sicherheitsgesetz, welches im Juli 2016 verabschiedet wurde. Dabei ging es um kritische Infrastrukturen, und wir gingen dafür auch ins Darknet.

Für den Fall, dass Sie nicht wissen, worum es sich handelt: Google & Co. kennen nur einen Teil des Internets, der Zugang ins Darknet oder auch ins Deep Web, die Begriffe sind nicht einheitlich, bleibt deswegen für viele Nutzer im Verborgenen. Um dorthin zu kommen, benötigt ein Nutzer eine bestimmte Anonymisierungssoftware, etwa „TOR" (engl. für The Onion Router). Die „Onion" – Zwiebel – steht sinnbildlich dafür, dass jemand, der das Netzwerk überwacht, wie bei einer Zwiebel nur die äußeren Schalen betrachten kann, aber nicht den Kern, genauer: den eigentlichen User. Das Entdeckungsrisiko von Verbrechern im Darknet ist folglich nahe null.

Wer ins Darknet gelangt, dem eröffnet sich ein bizarrer Basar rund ums das Illegale. Die sogenannten Peer-to-Overlay Netzwerke, sie beruhen auf der gleichen Technologie wie das Internet, kennen zum Beispiel Foren für Straftaten aller Art. Es werden etwa Summen für bestimmte kriminelle Aktionen ausgehandelt und man trennt sich nach einem Vertragsabschluss schnell wieder. Nach dem Ausführen der Straftat fließt dann das Geld.

Mein Kunde wollte wissen, ob personenbezogene Daten, wie Anschrift, Kreditkarten-Nummern, User und Passwörter, im Darknet einfach und schnell zu holen sind – trotz starker und aktueller Firewalls in den firmeneigenen Systemen. Hintergrund war die Veröffentlichung solcher sensibler Daten im Falle des Seitensprungportals „Ashley Madison" im Sommer 2015. Eine Hackergruppe hatte seinerzeit die Veröffentlichung der Daten angedroht, sofern die Internet-Seite nicht umgehend vom Betreiber geschlossen wird, und bereits erste Daten für Jeden sichtbar online gestellt. Weil „Ashley Madison" nicht reagierte, kam es zur

Bei der Auswahl ihrer Passwörter sind viele Nutzer sehr ideenlos. Das hilft Kriminellen, wie diese Darknet-Auflistung zeigt.

privat

Veröffentlichung von weit über 32 Millionen Userdaten aus dem Darknet. Die Datenbank enthielt alle User mitsamt persönlichen Daten und unter anderem auch deren sexuelle Vorlieben. Ein weiterer Fall war die vollumfängliche Veröffentlichung einer Kreditkarten-Datenbank mit dem Tagesumsatz am 28. Juni 2015 von rund 98.000 US-Dollar, einschließlich Vor- und Zunamen, Geodaten, Adressen und dem Datum der letzten Überweisung sowie dem am Stichtag überwiesenen Betrag.

Im Falle meines Auftragsgebers habe ich nicht nur interne Dokumente im Darknet gefunden, wie zum Beispiel Arbeitsverträge, Geheimhaltungsverpflichtungen oder „PayPal"-Zugänge, sondern ich fand auch viele Dokumente im Klartext abgespeichert vor – trotz funktionierender Sicherheitsvorkehrungen und dem Einsatz von Passwörtern.

Sie fragen sich jetzt bestimmt: Wie kann das passieren? Die Antwort ist einfach und erschreckend zugleich: Viele Passwörter werden nur mit einem „MD5 Hash" gespeichert. Dieses technische Verschlüsselungsverfahren darf nicht mehr als sicher gelten! In unserem Seminar hatten wir in nur zwei Wochen rund 15 Millionen Passwörter entschlüsselt, welche diese kryptographische Methode verwenden. Genauere Angaben hierzu möchte ich aus Sicherheitsgründen allerdings nicht machen.

Viele weitere, sehr bedenkliche Dinge habe ich im Darknet gefunden, zum Beispiel von DAX notierten Unternehmen. Mit den leicht gewonnenen Kundendaten hätte ich zum Beispiel ohne Probleme im Internet auf Shoppingtour gehen können.

Was hilft gegen solche Lücken und was schützt vor dem Darknet?

Mein erster Tipp: Wechseln Sie so schnell wie möglich zu einer moderneren Verschlüsselungsfunktion. Mein zweiter Tipp betrifft die gewählten Passwörter. Selbst für mich als erfahrenen IT-Sicherheitsberater war die Auswahl der meist benutzten Passwörter von Usern erschreckend – siehe nebenstehende Bildschirmkopie. Allein 5.882 Mal wurde das Passwort „123456" benutzt und 2.486 Mal das Wort „password"! Dritter Tipp: Verwenden Sie für unterschiedliche Anwendungen unterschiedlich sichere Passwörter.

Gegen so massive Datenverluste, wie gerade beschrieben, wirken oft schon einfache IT-Sicherheits-Mechanismen und -Strukturen. Und sollten Sie Zweifel haben, ob Ihre Daten sicher sind: Lassen Sie sich kompetent beraten. Das ist allemal günstiger als ein Datenklau über das Darknet. Und wenn Sie mehr IT-Sicherheit haben wollen, sollten Sie nicht nur alle Ihre Prozesse rund um die IT überprüfen. Hilfreich sind dann unter anderem Penetrationstests von außen, das sind gezielte, koordinierte Angriffe auf Ihr Unternehmensnetzwerk mit anschließender Analyse der Sicherheitslücken.

IHK

Marcel Jordan
EDV-Sachverständigen- und Forensikbüro JORDAN, Sinntal-Altengronau

INFO

Marcel Jordan ist nicht nur „M-Net"-Vertriebspartner in der Region, sondern er ist unter anderem auch Mitglied in der „Allianz für Cyber-Sicherheit" beim „Bundesamt für Sicherheit in der Informationstechnik". Außerdem ist er Mitglied im „EDV Gerichtstag e.V.", in der „Deutschen Sachverständigen Gesellschaft GmbH" (DESAG) sowie im „Berufsfachverband für das Sachverständigen- und Gutachterwesen e.V." Er ist durch den TÜV SÜD zertifiziert in Informationssicherheit nach ISO/IEC 27001. ●