24.01. 2019

Tipps zur Datensicherheit: „Wer sicher sein will, muss sich selbst schützen“

Von PPS

Bild Rechte
Matrix42

Ein Statement von Sergej Schlotthauer, VP Security bei Matrix42, zum Politiker- und Promi-Hack

(Luzern)(PPS) **Glauben Sie daran, dass es wirklich ein Schüler war, der massenhaft Daten von Prominenten und Politikern gehackt hat und als Twitter-Adventskalender der Öffentlichkeit präsentierte? Bei der Vernehmung konnte der Beschuldigte nicht einmal eine Zwei-Faktor-Authentifizierung umgehen, was jedoch nach Kenntnissen der Behörden Bestandteil des Angriffes war. Wahrscheinlicher ist, dass mehrere Hacker an dem Angriff beteiligt waren, und die endgültige Wahrheit wohl im**

Dunkeln bleibt. Es ist einfach extrem schwer, die wahren Täter zu fassen und die Verhinderung solcher Angriffe ist von Seiten des Staates und der Behörden nahezu unmöglich. Wer sicher sein will, muss sich selbst schützen. Aber welcher Schutz ist der richtige?

Da sind zunächst einmal die Passwörter – immer wieder wird davor gewarnt, zu einfache Passwörter zu verwenden oder achtlos mit ihnen umzugehen. Dazu gibt es auch schon seit Jahren eine BSI-Richtlinie, die man problemlos im Internet finden kann. Dennoch muss man wieder verwundert lesen, dass 123456 immer noch das am meisten verwendete Passwort ist – wie kann das sein? Das Problem ergibt sich wahrscheinlich genau aus den Empfehlungen des BSI, denn ein Passwort soll komplex sein und verschiedenen Zeichenformen beinhalten. Damit wird es aber schwer, sie auswendig zu lernen, zumal man heutzutage viele verschiedene benötigt. Man muss sie also irgendwo aufschreiben, womit dann aber das nächste Problem beginnt. Wie sorge ich dafür, dass die Passwörter zwar verfügbar sind, wenn man sie braucht, jedoch nicht von Dritten entwendet werden können? Moderne Passwort-Manager können hier Abhilfe schaffen. Sie funktionieren wie ein Safe auf dem Rechner oder in der Cloud. Man muss sich nur ein Passwort merken, mit dem man den Safe öffnen kann. Alle anderen Passwörter befinden sich sicher verschlüsselt im Passwort-Manager.

Die zweite Sicherheitsmaßnahme, die immer wieder angesprochen wird, ist die Verschlüsselung. Sie verhindert zwar nicht, dass Daten gestohlen werden, aber sie machen sie immerhin für den Datendieb unbrauchbar. Der Aufwand, moderne Verschlüsselungscodes zu knacken, ist für den 08/15-Hacker viel zu hoch. Dennoch kommt Verschlüsselung viel zu selten zum Einsatz – das betrifft sowohl den Privat- als auch den Geschäftsbereich. Aber warum eigentlich? Hier spielt wohl die Bequemlichkeit des Menschen eine große Rolle. Die am weitesten verbreitete Verschlüsselungsmethode ist die Container-Verschlüsselung. Sie macht es nötig, einen Container zu definieren, anzulegen und ein Passwort dafür zu generieren. Alle Daten, die in den Container gelegt werden, werden verschlüsselt. Werden sie wieder gebraucht, muss man den Container jedes Mal mit Hilfe des Passworts öffnen. Das bedeutet, dass zusätzliche lästige Arbeitsschritte nötig sind, und zwar jedes Mal, wenn man Daten verschlüsseln oder entschlüsseln will. Und zusätzliche Passwörter kommen auch wieder zur Sammlung hinzu. Aber wenn es doch ratsam ist, sowieso alles zu verschlüsseln, warum braucht es dann den Container? Warum verschlüsselt man nicht alle Daten einfach beim ganz normalen Speichervorgang? Dateibasierte

Verschlüsselungslösungen oder auch „On-the-fly Verschlüsselung“ machen genau das, ohne dass zusätzliche Arbeitsschritte nötig sind. Man identifiziert sich einmal und die Daten sind immer zugriffsbereit. Verwendet man dazu noch eine Zwei-Faktor-Authentifizierung, ist man künftig richtig sicher. Durch die einfache Handhabung sind sie sowohl für private als auch für geschäftliche IT-Nutzer empfehlenswert. Für geschäftlich genutzte Daten kommt außerdem hinzu, dass die EU-DSGVO die Verschlüsselung personenbezogener Daten vorschreibt – dieses Problem wäre also auch gleich mitgelöst.

Im Geschäftsbereich kommt noch ein dritter wichtiger Grundsatz dazu. Es gilt die Vorgabe, dass nur ein gemanagter Rechner ein sicherer Rechner ist. Alle geschäftlichen IT-Devices gehören zwingend ins Netzwerk- und Sicherheitsmanagement des Unternehmens. Am sichersten sind Unternehmen und Organisationen, wenn sie eine Lösung einsetzen, die Management und Sicherheit aller Endpoints aus einer Hand bietet.

Bild: Sergej Schlotthauer

Pressekontakt:

Matrix42 Helvetia AG
Habsburgerstrasse 52A
6003 Luzern

Matrix42
Gisela Dauer
Senior Communication Manager
Tel: +49 69 66773-8378
Mobile: + 49 172 274 11 51
Fax: +49 69 66773-8380
gisela.dauer @ matrix42.com

Kategorie
IT & Software & Neue Medien
