Thema: **Datenskandal aus dem Kinderzimmer – So hätte er vermieden werden können**

Beitrag: 1:46 Minuten

Anmoderationsvorschlag: Auch, wenn das Jahr 2019 noch jung ist, hat es schon seinen ersten Skandal: Einen Daten-Skandal! Am 3. Januar wurde bekannt, dass jemand den ganzen Dezember über persönliche Daten von deutschen Politikern und Prominenten veröffentlicht hat, in einer Art "Adventskalender". Mittlerweile hat ein 20-jähriger gestanden, hinter dem Datenklau zu stecken. Bei den gestohlenen Daten handelt es sich vor allem um Telefonnummern und Privatadressen von Politikern und Prominenten. Von solchen Datenskandalen sind allerdings bei weitem nicht nur Prominente betroffen – auch Otto Normalbürger kann es erwischen. ABER: Man kann sich dagegen wehren! Wie? Das weiß Jessica Martin!

Sprecherin: Fakt ist: So ein Datenklau kann in der Tat jeden treffen. Der Digitalverband Bitkom hat letztes Jahr festgestellt, dass jeder zweite Internet-Nutzer in Deutschland schon mal Opfer von Cyberkriminalität geworden ist. Schuld sind aber auch wir selbst, sagt Thomas Uhlemann vom Internet-Sicherheitsanbieter ESET.

O-Ton 1 (Thomas Uhlemann, 18 Sek.): „Wir machen es als Nutzer den Angreifern noch viel zu leicht. Also unsere Daten, die wir zum Beispiel in Cloud-Speichern ablegen – ob das Dropbox ist, Google Drive etc. – legen wir dort nicht verschlüsselt ab. Oder eben auch die Passwörter, die wir verwenden, die sind leider extrem schwach, sind Wörter aus dem Wörterbuch und können so dementsprechend leicht geknackt werden …“

Sprecherin: Ein gutes Passwort sollte mindestens acht Zeichen lang sein…

O-Ton 2 (Thomas Uhlemann, 14 Sek.): „…und bei wichtigen Aktionen wie eben Verschlüsselungen oder dem WLAN-Passwort zu Hause, sollte es schon mindestens 20 Zeichen haben. Und es sollte auch immer eine Kombination sein aus Zahlen, Buchstaben und Sonderzeichen, Satzzeichen und so weiter….“

Sprecherin: Das Problem bei wirklich sicheren Passwörtern ist aber, dass man sich die nicht merken kann…

O-Ton 3 (Thomas Uhlemann, 30 Sek.): „Und deswegen empfehlen wir von ESET auch einen Passwortmanager zu verwenden, wie er zum Beispiel in unserer ESET Smart Security Premium enthalten ist, und der mir auch die Passwörter generieren kann. Das heißt, ich muss mir gar nicht erst mal eine halbe Stunde ein Passwort überlegen, ein super komplexes, das heißt, der generiert ein Passwort, speichert das, verschlüsselt das und dann in dem Moment, wo ich dann die Dienste aufrufe, fügt er mir die Passwörter automatisch ein. Und das eben nicht nur am Rechner, sondern auch als App auf iOS oder Android.“

Sprecherin: Mit ein paar unkomplizierten Verschlüsselungslösungen hätte der jüngste Datenskandal also problemlos verhindern werden können.

O-Ton 4 (Thomas Uhlemann, 10 Sek.): „…und mit dem Bewusstsein, dass es die technologischen Lösungen gibt und dass meine Daten als das Öl des 21. Jahrhunderts betrachtet werden – und dann sollte ich sie auch dementsprechend schützen. ...“

Abmoderationsvorschlag: Ausführliche Infos rund um Ihre Internet-Sicherheit finden Sie auch im Internet unter eset.de. Dort finden Sie auch jede Menge Möglichkeiten zur Daten-Verschlüsselung und zu sicheren Passwörtern!

Thema: **Datenskandal aus dem Kinderzimmer – So hätte er vermieden werden können**

Interview: 2:19 Minuten

Anmoderationsvorschlag: Auch, wenn das Jahr 2019 noch jung ist, hat es schon seinen ersten Skandal: Einen Daten-Skandal! Am 3. Januar wurde bekannt, dass jemand den ganzen Dezember über persönliche Daten von deutschen Politikern und Prominenten veröffentlicht hat, in einer Art "Adventskalender". Mittlerweile hat ein 20-jähriger gestanden, hinter dem Datenklau zu stecken. Bei den gestohlenen Daten handelt es sich vor allem um Telefonnummern und Privatadressen von Politikern und Prominenten. Von solchen Datenskandalen sind allerdings bei weitem nicht nur Prominente betroffen – auch Otto Normalbürger kann es erwischen. ABER: Man kann sich dagegen wehren! Wie? Das weiß Thomas Uhlemann vom Internet-Sicherheitsanbieter ESET, hallo!

Begrüßung: „Hallo!“

1. ***Herr Uhlemann, zunächst einmal: Kann so ein Datenklau echt JEDEN treffen?***

O-Ton 1 (Thomas Uhlemann, 19 Sek.): „Leider – und auf jeden Fall, ja! Also der Digitalverband Bitkom hat zum Beispiel 2018 erst festgestellt, dass jeder zweite Internet-Nutzer in Deutschland schon mal Opfer von Cyberkriminalität geworden ist und einem Viertel der Nutzer sind persönliche Daten auch dabei gestohlen worden, die dann illegal genutzt oder eben an Dritte weitergegeben oder verkauft wurden.“

2. ***Wie kommt es denn zu solchen Zwischenfällen?***

O-Ton 2 (Thomas Uhlemann, 21 Sek.): „Ja, das geht bei der Handhabung los. Also, wir machen es als Nutzer den Angreifern noch viel zu leicht. Also unsere Daten, die wir zum Beispiel in Cloud-Speichern ablegen – ob das Dropbox ist, Google Drive etc. – legen wir dort nicht verschlüsselt ab. Oder eben auch die Passwörter, die wir verwenden, die sind leider extrem schwach, sind Wörter aus dem Wörterbuch und können so dementsprechend leicht geknackt werden.“

3. ***Wie sollte denn ein gutes Passwort aussehen?***

O-Ton 3 (Thomas Uhlemann, 18 Sek.): „Ein gutes Passwort sollte also mindestens acht Zeichen lang sein und bei wichtigen Aktionen wie eben Verschlüsselungen oder dem WLAN-Passwort zu Hause, sollte es schon mindestens 20 Zeichen haben. Und es sollte auch immer eine Kombination sein aus Zahlen, Buchstaben und Sonderzeichen, Satzzeichen und so weiter….“

4. ***Die kann man sich doch aber gar nicht mehr merken!***

O-Ton 4 (Thomas Uhlemann, 37 Sek.): „Ja, leider ist das so, dass man sich das schlecht merken kann – gerade bei der Masse an Diensten, wofür wir heute alles ein Passwort brauchen. Und deswegen empfehlen wir von ESET auch einen Passwortmanager zu verwenden, wie er zum Beispiel in unserer ESET Smart Security Premium enthalten ist, und der mir auch die Passwörter generieren kann. Das heißt, ich muss mir gar nicht erst mal eine halbe Stunde ein Passwort überlegen, ein super komplexes, das heißt, der generiert ein Passwort, speichert das, verschlüsselt das und dann in dem Moment, wo ich dann die Dienste aufrufe, fügt er mir die Passwörter

automatisch ein. Und das eben nicht nur am Rechner, sondern auch als App auf iOS oder Android."

5. ***Als Fazit kann man also sagen, dass der jüngste Datenskandal durchaus auch hätte verhindert werden können?***

O-Ton 5 (Thomas Uhlemann, 27 Sek.): „Ja, auf jeden Fall! Also mit dem Stand der Technik, den wir nicht nur letztes Jahr, sondern auch jetzt haben, hätte man das auf jeden Fall verhindern können. Da gibt's verschiedenste Verschlüsselungslösungen - ob die ESET Smart Security Premium für Heimanwender oder die ESET Endpoint Encryption für die Unternehmen heißt oder viele, viele andere auch – und natürlich hätte man es verhindern können mit dem Bewusstsein, dass es die technologischen Lösungen gibt und dass meine Daten als das Öl des 21. Jahrhunderts betrachtet werden – und dann sollte ich sie auch dementsprechend schützen."

Thomas Uhlemann von ESET über den jüngsten Datenskandal und wie man ihn hätte vermeiden können! Vielen Dank für das Gespräch!

Verabschiedung: „Ich danke Ihnen!"

Abmoderationsvorschlag: Ausführliche Infos rund um Ihre Internet-Sicherheit finden Sie auch im Internet unter eset.de. Dort finden Sie auch jede Menge Möglichkeiten zur Daten-Verschlüsselung und zu sicheren Passwörtern!