Hackerparadies Österreich? End User als Schlüsselfaktor

30. Jan 2017 **Recht**

©PHH

Wien. Um Trends beim Cybercrime und effektive Gegenmaßnahmen ging es jetzt bei einer Diskussion von PHH Rechtsanwälte. Im Fokus war die IT-Sicherheit kleiner wie großer Unternehr Der End User ist dabei der Schlüssel.

Stefan Prochaska, Partner bei PHH Rechtsanwälte diskutierte mit Peter Kleissner (Ex-Hacker und Szenekenner), Mathias Preuschl (PHH Rechtsanwälte), Walter Unger (Abwehramt), Hubert Wack (ITSV GmbH) und Benjamin Weissmann (EY).

Die Situation

„Die Opfer von Cybercrime sind meist extrem sorglos. Sie schaffen sich zwar ein Anti-Virus-Programm an, aber die meisten Passwörter sind offen zugänglich. Das ist so, als ob ich einen Tresor habe und den Schlüssel dazu da an einen Haken hänge“, sagt Preuschl. Benjamin Weissmann, Geschäftsführer der Forensic und IT-Security bei EY: „Die meisten Menschen wählen Passwörter, die sie sich gut merken können und verwenden viel zu lange diesselben Passwörter. Das macht es Angreifern leicht.“

Kleissner sieht den Schwachpunkt hingegen bei veralteter Software: „90 bis 95% aller Hacker-Attacken könnten verhindert werden, w die Unternehmen ihre Betriebssysteme wie Software up to date hielten.“

„Die Täter kommen von überall, wir haben schon die Namen von über 500 Hackergruppierungen identifiziert“, berichtet Unger vom Abwehramt. Neben kriminellen Organisationen gebe es auch sogenannte Staatshacker, die im Auftrag eines Staates Spionage betreil „Es ist schwierig die Täter zu fassen, weil diese international tätig sind“, so Unger.

Die last line of defence ist immer der End User. Und gerade dieser ist oft ein Risikofaktor in der Abwehrkette, berichtet Weissmann au seiner Praxis. Die klassische Vorgangsweise, wenn ein Virus auf einem Computer gefunden werde, sei etwa, diesen vom Netz zu neh und neu aufzusetzen. Ob noch andere Geräte infiziert sind, werde meist gar nicht oder viel zu spät überprüft. „Viele Mitarbeiter denke nicht daran, dass andere ebenfalls betroffen sein könnten. So verlieren IT-Abteilungen wertvolle Zeit“, so Weißmann.

Außerdem verursachen oft die Mitarbeiter selbst ein Datenleck, etwa indem sie wichtige Daten gar nicht verschlüsseln oder die Passwörter allgemein zugänglich abspeichern. Und auch Ex-Mitarbeiter können ein Risiko sein. „Manchmal sind Mitarbeiter wütend, v sie das Unternehmen verlassen und nehmen Daten aus Rache mit“, so Preuschl.

Risiko minimieren durch Awareness

Um gegen Cybercrime gerüstet zu sein, brauche es ein geschärftes Bewusstsein für die Problematik, so die Experten. „Cybercrime ist nicht nur Chefsache, sondern betrifft alle Mitarbeiter im Unternehmen“, so Wackerle und betont: „Für das Verhalten gibt es keine Lösungen, da hilft nur üben, üben, üben.“ Führungskräften kommt dabei eine Vorbildfunktion zu. „Wenn der Chef schleißig im Umgang den Daten ist, dann werden es auch die Mitarbeiter sein“, so Weissmann.

Opfer der derzeit aktuellen Erpressungstrojaner-Wellen sollten jedenfalls auf keinen Fall Lösegeld für ihre Daten zahlen, mahnt Preus Denn das erpresste Geld fließe nur in den weiteren Aufbau von kriminellen Strukturen. Statt dessen rät Preuschl, die Attacke anzuzeig die Sicherheitslücken zu schließen und sofort die Betroffenen zu informieren. Das Unternehmen müsse dabei ruhig und koordiniert kommunizieren. Je professioneller ein Unternehmen mit der Situation umgeht, desto besser, sagt Weißmann.

Link: **PHH**

Weitere Meldungen:

1. **Unternehmen müssen sich auf EU-Datenschutzregeln vorbereiten**
2. **Bis zu 10 Mio. Euro Strafe für Zögern nach Cyberattacke**
3. **Frehsfields empfiehlt Unternehmenskäufern einen zweiten Blick auf die IT-Sicherheit**
4. **Freshfields: Das Wiener Büro lässt den Guardian Angel los, bei mittlerer Gefahrenlage**
5. **Härtetest für die neue Kronzeugen-Regelung: Wiener Kammer-Vize Stefan Prochaska informiert auf Facebook**

« **Bucerius will Österreichs Anwälten Soft Skills vermitteln**

Wo Gefahr durch Falschgeld in Österreich am größte