



## Cybercrime: Prävention lohnt sich

Die Zahl der von Internetkriminalität Betroffenen steigt weiter. Jeder Betrieb - unabhängig von der Unternehmensgröße - kann von Cyber-Angriffen getroffen werden.

06.07.2022, 8:57



Paul Schussmann, Gründer von SecAttack und Martin Heimhilcher, Spartenobmann Information & Consulting, gaben Tipps zur Abwehr von Cyberkriminalität. © WKW/ZIEGELWANGER

Paul Schussmann leitet ein Unternehmen, das sich auf Sicherheitstests in Sachen Hackerangriffe spezialisiert hat. Gemeinsam mit Martin Heimhilcher, Spartenobmann Information und Consulting, informierte er, wie Hacker versuchen, Link zu öffnen“, so Schussmann. Das Schema solcher Angriffe sei immer das gleiche: Personen kontaktieren, Vertrauen aufbauen, manipulieren, Stress aufbauen, sein Spiel mit Emotionen treiben und meist öffnen diese Personen dann die gesendete Datei und schon breitet sich ein Virus im System aus, oder Ransomware verschlüsselt die Daten, damit Lösegeld verlangt werden kann.

### Oberstes Gebot: Mitarbeiter schulen

„Oft sind die gefährlichen Links schwer zu identifizieren. Man bekommt viele Mails pro Tag. Man kann Mitarbeitern keinen Vorwurf machen, wenn sie darauf reinfallen“, sagt Schussmann. Wenn das passiert, dann helfen die beste Firewall und andere technische Sicherungen nichts. „Was nützt eine coole Alarmanlage, wenn Türen und Fenster weit offen sind?“, fragt Schussmann. Am besten man kombiniert Schulungen mit technischer Prävention. Das Bewusstsein zu schaffen, bei welchen Anrufen oder Mails es sich um eine Attacke handeln könnte, sei eine der wichtigsten Präin die Netzwerke von Betrieben zu gelangen und was man dagegen tun kann. „Das leichteste Weg ist, das schwächste Glied der Sicherheitskette zu identifizieren und dann anzugreifen. Die beste Firewall nützt nichts, wenn man einen Mitarbeiter dazu bringt, einventionsmaßnahmen. Heimhilcher weiß, dass es für jeden Betrieb wichtig ist, vorbereitet zu sein. „Die Zahl der Cyber-Angriffe, von denen wir wissen, steigt seit Jahren - dazu kommt eine hohe Dunkelziffer. Ein-Personen-Unternehmen sind ebenso betroffen wie große Firmen. Daher ist es so wichtig, den Kriminellen den Zugriff so schwer wie möglich zu machen.“ Leider fehle in vielen Betrieben die Expertise, und oft entdeckte man die Attacke viel zu spät. Gerade für kleine Betriebe sei es daher wichtig, einen IT-Spezialisten zu haben.

## Wenn der Angriff doch passiert

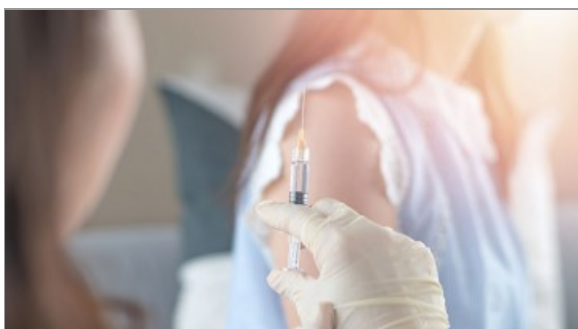
„Meist ist man im ersten Moment überfordert, wenn man Opfer eines Cyber-Angriffs wird. Verständlich, wenn das IT-System lahmgelegt wird, Daten verloren gegangen sind und von einem normalen Betrieb keine Rede sein kann“, so Heimhilcher. Genau deshalb ist es im Fall der Fälle wichtig, schnell und unbürokratisch Hilfe zu bekommen. Entweder bei seinem IT-Experten oder auch bei der Cybersecurity-Hotline der Wirtschaftskammer, die dann jemanden vermittelt. „Ganz wichtig ist es auch, die Angriffe immer zur Anzeige zu bringen, um die Chance zu erhöhen, die Täter zu erwischen“, so Heimhilcher abschließend.

## Das könnte Sie auch interessieren



### Service für alle Fälle

Verlässliche Informationsquelle, Ansprechpartner und Anlaufstelle: Das Service der WK Wien steht den Wiener Betrieben in allen Unternehmenslagen als zuverlässiger Wegbegleiter zur Seite. [➤ mehr](#)



### Kostenlose HPV-Impfung für junge MitarbeiterInnen im Betrieb

Aufgrund aktueller Entwicklungen können wir Ihnen mitteilen, dass die kostenlose HPV-Impfaktion auf den betrieblichen Bereich ausgeweitet werden kann. [➤ mehr](#)



## Wenn Familienmitglieder im Betrieb aushelfen

Arbeiten Angehörige im Betrieb mit, wird immer im Einzelfall beurteilt, ob dadurch ein Dienstverhältnis mit allen daraus folgenden Konsequenzen begründet wird. Was grundsätzlich zu beachten ist.

➤ mehr