
Foto: Erath

Jörn Weber ermittelt im Auftrag von Unternehmen.

„Für alle Krisenfälle muss es einen Ablaufplan geben"

Jörn Weber ist Privatermittler. Mit seinem Unternehmen corma hat sich der ehemalige Polizist auf Wirtschaftsdelikte spezialisiert.

Herr Weber, worauf haben es Betrüger abgesehen, wenn Sie via Internet angreifen?
Jörn Weber: Letztlich immer auf Geld. Das steht an erster Stelle. Gerade bei Angriffen, die die breite Masse treffen wie die Ransomware-Angriffe. Dabei werden Daten verschlüsselt und nur gegen Zahlung wieder freigegeben. Bei gezielten Angriffen geht es auch um Daten.

Wie können sich Unternehmen bestmöglich gegen Cyber-Attacken wappnen?
Weber: Ziel ist, es den Hackern so schwer wie möglich zu machen. Da gibt es einige Optionen. Die Schad-Software gelangt meist per E-Mail in das Netzwerk des Opfers. Ein Virenschutz lokal am Rechner reicht aber schon lange nicht mehr aus. Wir arbeiten beispielsweise mit einem Dienstleister zusammen, der alle unsere E-Mails auf Schad-Software scannt, bevor sie auf unseren Rechnern landen. Seit wir diese Firma beauftragt haben, ist kein Virus mehr bei uns angekommen. Lediglich harmlose Spammails kommen – wenn sie gut gemacht sind – ab und zu durch.

>> Ich will auf unseren Firmenrechnern keine Privatsachen haben. <<
Jörn Weber, corma GmbH, Brüggen

Werden da auch Mails gescannt, die in privaten Postfächern auf dem Rechner landen?
Weber: Nein. Aber unsere Mitarbeiter dürfen mit den Firmenrechnern nicht privat surfen oder private Mails verschicken. Mir geht es nicht um die Arbeitszeit. Meine Mitarbeiter können ihre Handys für diese Sachen nutzen, auch während der Arbeitszeit. Ich will nur auf unseren Rechnern keine Privatsachen haben.

Viele Maßnahmen greifen nur bei Schad-Software, die an die breite Masse gerichtet wird. Es gibt aber doch auch ganz gezielte Angriffe.
Weber: Zum Beispiel den sogenannten CEO-Fraud. Diese Masche ist mittlerweile ein riesiges Problem und hat schon bei vielen Unternehmen

>> Sicherheit kostet im ersten Moment nur Geld. <<
Jörn Weber, corma GmbH, Brüggen

sehr gut geklappt. Aber auch da gibt es Schutzmaßnahmen, zum Beispiel, indem die Mitarbeiter gezielt geschult werden.

Und wenn doch einmal ein Angriff durchkommt?
Weber: Für alle potenziellen Krisenfälle muss es im Unternehmen Ablaufpläne geben, die schnell greifen. Denn eine Krise meldet sich ja nicht vorher an, sie ist ganz plötzlich da. Die Mitarbeiter kommen montags ins Büro und merken plötzlich, dass das Firmennetzwerk mit einem Virus befallen ist. Da hat man keine Zeit, lange zu überlegen, was jetzt zu tun ist. Wenn uns ein Unternehmen beauftragt, seine Unternehmenssicherheit zu prüfen, dann entwickeln wir auch gemeinsam Pläne für den Ernstfall. Es sollte auch nicht nur das Kernunternehmen gesichert sein, sondern auch alle Dienstleister und Zulieferer, die wichtige oder geheime Informationen bekommen.

Welche Rolle spielt der Faktor Mensch in Sachen Sicherheit?
Weber: Eine große. Die Mitarbeiter müssen entsprechend sensibilisiert werden. Zum Beispiel dafür, keine Auskünfte zu erteilen, ob die Geschäftsführung gerade im Urlaub oder auf dem Golfplatz ist. Man muss ihnen erklären, was zu tun ist, wenn eine E-Mail ankommt, die einen komischen Eindruck macht, und deutlich machen, dass die Mitarbeiter auch beim Vorstand noch einmal nachfragen dürfen, ohne dass es Ärger gibt. Es geht auch darum, was das Unternehmen selber veröffentlicht und was zum Beispiel Familienangehörige – häufig unbewusst – in sozialen Netzwerken posten.

Wie hoch ist denn die Wahrscheinlichkeit, nach einem Angriff die Täter zu erwischen?
Weber: Täter machen immer Fehler, aber es erfordert ein hohes Maß an Ermittlungsarbeit, sie auch zu überführen. Die Hacker operieren in der Regel aus dem Ausland. Bis ein internationales Rechtshilfeersuchen gestellt wurde, sind sie und meist auch die Beute weg. Schnell sein ist also alles. Womit wir wieder bei den Notfallplänen wären.

Warum unterschätzen viele Unternehmen die Gefahr, die durch das Netz kommt?
Weber: Weil die Unternehmer sich mehr um die Angelegenheiten kümmern, die Geld einbringen. Sicherheit kostet im ersten Moment nur Geld. Auch wenn zum Beispiel die E-Mail-Sicherheit, über die wir eben sprachen, meiner Meinung nach nicht die Welt kostet. Den Firmen muss klar sein, dass letztlich mit der Investition Schaden abgewendet wird, auch ein Imageschaden. Und vielleicht wird durch einen guten Sicherheitsplan im Ernstfall auch Geld zurückgeholt. Das Problem ist nur, dass man diese Eventualitäten nicht beziffern kann.

Nina Mützelburg

WAS IST ...

... Ransomware?
Ransomware wird auch als Erpressungstrojaner oder Kryptotrojaner bezeichnet. Das Prinzip ist einfach: Eindringlinge verschaffen sich Zutritt zu einem Netzwerk, zum Beispiel durch einen verseuchten Mail-Anhang. Dann verschlüsseln sie alle Daten, die sich auf dem Rechner befinden. Für die Entschlüsselung benötigt der Nutzer einen Code. Die Erpresser fordern eine Lösegeldsumme für die Herausgabe des Codes.

... ein Botnetz?
Ein Botnetz ist ein Online-Netzwerk aus privaten Computern, die erst infiziert und dann zusammengeschlossen werden. Prinzipiell kann jeder Rechner Teil eines solchen Netzwerks werden und somit von Kriminellen ferngesteuert werden. Ein derartig infiziertes System verschickt so beispielsweise massenhaft Spammails an alle Kontakte in der Mail-Liste und infiziert andere Computer.

... eine Ddos-Attacke?
Ddos ist die Abkürzung für „Denial of Service", also „Dienstblockade" oder „Dienstverweigerung". Dafür manipulieren Hacker Maschinen, die massenhaft Anfragen an speziell ausgewählte Server stellen. Unter dieser Last brechen die Server zusammen. Die dazugehörigen Websites sind nicht mehr erreichbar.