Cyber Security – Vorbeugen ist besser

Interview mit **Pascal Bergmeier**, Direktion Kriminalität des Polizeipräsidiums Bonn

Verhaltensprävention hat das beste Kosten-/Nutzenverhältnis

Aufgabe der Polizei ist es, neben der Verfolgung von Straftaten auch Gefahren für die öffentliche Sicherheit oder Ordnung abzuwehren. Dazu gehört auch, durch Information und Schulung Präventionsarbeit zu leisten und somit Straftaten vorbeugend zu bekämpfen. Immer mehr Straftaten finden im Netz statt, sie werden unter dem Begriff „Cybercrime" zusammengefasst. Pascal Bergmeier, gelernter IT-Systemkaufmann und Betriebswirt, ist im Polizeipräsidium Bonn für Kriminalprävention, Opferschutz und Cybercrime zuständig. Er ist Teil eines großen Teams, das dafür sorgt, das Bewusstsein für Cybercrime und Cybersicherheit zu schärfen.

„Die Wirtschaft": *Herr Bergmeier, Sie sind für Kriminalprävention, Opferschutz und Cybercrime zuständig. Was müssen wir uns darunter genau vorstellen?*

Pascal Bergmeier: Die Prävention ist ein zentraler Beitrag zur Gewährleistung der Inneren Sicherheit. Das polizeiliche Ziel meiner Aufgabe ist es deshalb, Bürgerinnen und Bürger, Wirtschaft, Verbände, öffentliche Verwaltung und andere Aufgabenträger zu sicherheitsbewusstem Verhalten zu veranlassen. Die Cybercrime-Prävention informiert alle Interessengruppen über Erscheinungsformen der Kriminalität, polizeiliche Bekämpfungsziele, Gefährdungseinschätzungen und Opferrisiken. Der Hauptfokus der Aufgabe liegt dabei auf der Empfehlung zu tatreduzierenden Verhaltensweisen.

Wie groß ist denn die Bedrohung durch Cyberkriminalität?

Dazu nenne ich gerne einige Zahlen aus allgemein zugänglichen Statistiken. Im Jahr 2025 werden rund 75 Milliarden Geräte mit dem Internet verbunden sein – das Zehnfache im Vergleich zu 2016. Im April 2019 verzeichnete die Deutsche Telekom mehr als 40 Millionen tägliche Angriffe auf ungeschützte Rechner – sogenannte „Honey Pots". 2018 betrug die Zahl der Cybercrime-Opfer in Deutschland zirka 19 Millionen – 70 Prozent davon waren Unternehmen. Der Schaden lag bei etwa 61,4 Millionen Euro. Beliebte Cyber-Attack-Methoden sind „Social Engineering" (47 Prozent) und Mail (80 Prozent). 30 Prozent sind erfolgreich aufgrund von „menschlichem Versagen". Was sagt uns das? Es wird definitiv der

Mensch und nicht die Technik als Schwachstelle und Einfallstor angesehen. Deswegen liegt der Fokus auf verhaltensorientierten Ansätzen.

Die größte Schwachstelle im System sind also wir selbst, die Nutzerinnen und Nutzer?

So ist es. Nehmen wir zum Beispiel das sogenannte Social-Engineering. Private Daten und Informationen über Personen sind mittlerweile sehr leicht recherchierbar. Etwas mehr als die Hälfte der Menschheit – 3,9 Milliarden – besitzt einen Account bei Facebook, WhatsApp oder Instagram. Knapp 3,4 Milliarden Menschen verfügen über einen Google-Account. Auf beiden Plattformen werden persönliche Daten publiziert. Sicherlich bestimmen die Nutzer selbst, welche Daten sie öffentlich der Allgemeinheit zur Verfügung stellen, und wir nehmen auch in keiner Weise eine wertende Stellung gegenüber den beiden Unternehmen ein. Aber wir weisen darauf hin, welche Recherche- und eben auch Missbrauchsmöglichkeiten durch diese enorme Verbreitung bestehen.

Sie beraten auch kleine und mittlere Unternehmen. Worin besteht denn deren größte Herausforderung in Sachen Cyber Security?

Ein grundlegendes sowie aktuelles Informationstechnologisches Wissen ist für die Arbeit von kleinen und mittleren Unternehmen (KMU) zwingend notwendig. Es gilt, ein Risikobewusstsein zu wecken. Hierfür müssen wir mit den verantwortlichen Personen auf Augenhöhe kommunizieren. IT-Sicherheit muss ein wichtiger Punkt in der Unternehmenskultur sein und auf Führungsebene vorgelebt werden. Viele KMU ziehen Effizienz und Agilität dem IT- und Datenschutz vor und sehen Sicherheitsvorgaben als hinderlich anstatt als notwendig an. So langsam ändert sich dies jedoch, und das Management schreibt der IT-Sicherheit eine höhere Priorität zu. Dies zeigt beispielsweise die TÜV-Cybersecurity-Studie 2019. Diese Entscheidungsträger gilt es zu erreichen. Verhaltensprävention kostet nichts und hat somit das beste Kosten-/Nutzenverhältnis.

Können Sie ein paar typische Cyberbedrohungen für Firmen nennen – und was sie anrichten können?

Am häufigsten sehen wir Phishing oder Spear-Phishing (26 Prozent) und Ransomware (19 Prozent). Diese werden für Datendiebstahl oder Geldbetrug verwendet. Eine gefälschte E-Mail, von einer vermeidlich vertrauenswürdigen Quelle, soll auf eine Webseite leiten, welche Schadsoftware beinhaltet. Der Phishing-Ansatz ist abhängig vom Zufall: Eine Vielzahl an Mails wird versendet. Spear-Fishing hingegen ist sehr zielgerichtet. Social-Engineering dient meist als Vorreiter. Hier werden die angeblich vertrauenswürdigen Mails gezielt an Adressaten versendet. Entweder wird Schadsoftware direkt installiert, oder es wird zu einer bestimmten Handlung, zum Beispiel einer Geldüberweisung aufgefordert.

Und was meinen Sie mit „Ransomware"?

Das ist eine Art von Schad- bzw. Erpressersoftware, welche Änderungen auf dem betroffenen PC oder in dem betroffenen Netzwerk vornimmt. Entweder werden alle Daten verschlüsselt oder der Zugriff auf das komplette System blockiert. Diese Änderungen werden dann nur gegen Zahlung eines Betrages von den Tätern wieder rückgängig gemacht.

Was können KMU tun, um sich die Bedrohung bewusst zu machen und ihr zu begegnen?

Ein zu hundert Prozent sicheres System gibt es nicht und wird es auch niemals geben! IT-Sicherheit wird vorwiegend von den zwei Komponenten Technik und Verhalten bestimmt. Technik kann das Nutzerverhalten unterstützen, und das Nutzerverhalten unterstützt die Technik. Keine der zwei Komponenten sollte isoliert oder unabhängig von der anderen betrachtet werden. Informieren Sie sich, seien Sie kritisch bei Aufforderung zu Datenangaben, lesen Sie sich Dinge genau durch, öffnen Sie keine unbekannten Sachen, stellen Sie Rückfragen bei Unsicherheit, leben Sie IT- und Datenschutz vor. Zu allen Präventionshinweisen und Sicherheitsmaßnahmen können Ihnen das BSI, die Polizei, die IHK sowie Ihr Internetserviceprovider oder andere IT-Unternehmen wertvolle Hinweise und Informationen liefern.

Lothar Schmitz,
Wirtschaftsjournalist, Bonn

Ansprechpartner:

Polizeipräsidium Bonn

Bereich Cybercrime - Pascal Bergmeier
Telefon-Hotline: 0228 15-7676
E-Mail-Hotline: kkkpo.bonn@polizei.nrw.de
https://bonn.polizei.nrw/artikel/cybercrime-3
Als übergeordnete Behörde und Ansprechpartner für herausragende Verfahren unterstützt das:

Landeskriminalamt NRW Düsseldorf

Cybercrime-Kompetenzzentrum
Tel. 0211 939-4040
cybercrime.lka@polizei.nrw.de
https://lka.polizei.nrw/en/node/1173
Weiterer Ansprechpartner für Cyberkriminalität:

Staatsanwaltschaft Köln

ZAC (Zentrale Ansprechstelle Cybercrime Nordrhein-Westphalen)
Tel. 0221 477-4422 / zac@sta-koeln.nrw.de
https://www.sta-koeln.nrw.de/aufgaben/geschaefte-stak_1_zac/index.php