Gießener Anzeiger, 04.10.2017

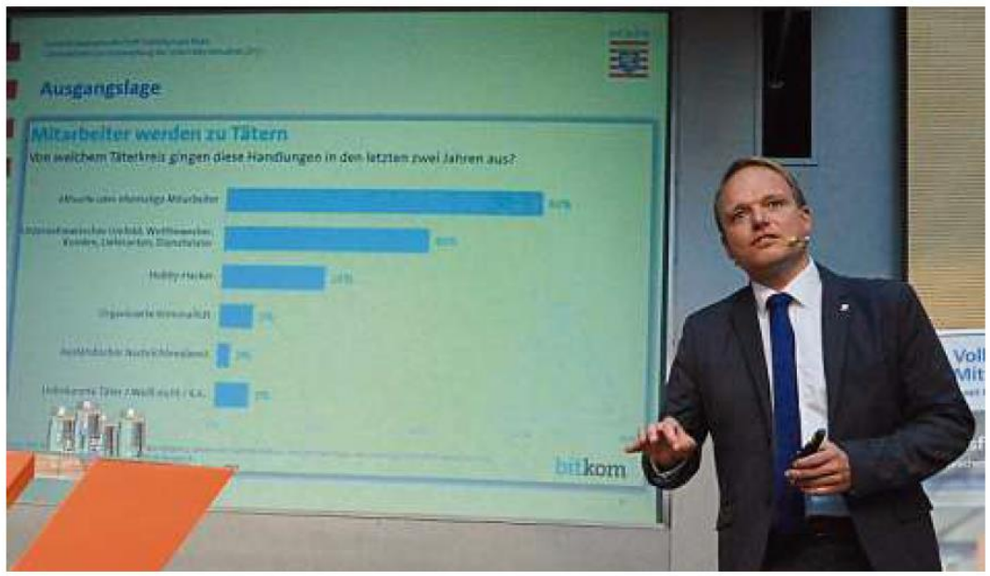
Betrüger sind sehr erfindungsreich

INTERNET Volksbank Mittelhessen klärt Unternehmen über Gefahren durch „Cybercrime" auf / System zum Schutz entwickelt

GIESSEN (sza). „Die Digitalisierung verändert alles. Sie bringt viel Neues, beschleunigt und entschlackt. Allerdings birgt sie auch neue Gefahren des Missbrauchs." Mit diesen Worte leitete Dr. Lars Witteck das MittelstandsKolleg der Volksbank Mittelhessen ein. Das übergeordnete Thema der Veranstaltung: „Cybercrime", die potenzielle Gefahr aus dem Netz. „Nicht nur große Unternehmen und Privatnutzer, sondern insbesondere auch die kleineren und mittleren Unternehmen werden angegriffen", richtete sich der Generalbevollmächtigte der Volksbank an die zahlreich erschienenen Gäste.

Mit welchen Maschen Cyberkriminelle vorgehen und wie gefährlich sie sind, diesen Problemen widmete sich Dr. Benjamin Krause in seinem Vortrag „Bedrohung durch Cybercrime – Option Strafanzeige". Der junge Staatsanwalt gehört zur Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT), die ihren Sitz in Gießen hat. „Es tut mir leid, dass ich das sagen muss. Aber es ist aus meiner Sicht schlimm, Sie zu sein. Denn Unternehmen wie Ihre sind das Hauptziel des Cybercrime", begann Krause mit einem Augenzwinkern, aber im Kern vollkommen ernst gemeint. Zwei Drittel aller Angriffe im vergangenen Jahr hätten sich gegen Unternehmen gerichtet, dabei sei deren Größe für die Täter völlig irrelevant gewesen. Gleiches galt auch für die Daten, die entwendet wurden. „Die Kriminellen haben sich, so muss man es sagen, alles genommen und ausgespäht, was sie bekommen konnten", erklärte der Experte. Zunächst zielten sie vor allem auf die Kommunikation ab. Wie groß die gesamtwirtschaftlichen Schäden durch diese Täter sind, zeigte Krause anhand einer Statistik des Bundesamtes. „Fast 55 Millionen Euro im Jahr kosten diese Angriffe und Verbrechen. Darunter fallen nicht nur die Schäden, die sie anrichten", berichtete der Staatsanwalt.

Andreas Kötter



Staatsanwalt Dr. Benjamin Krause zeigt die größten Unsicherheitsfaktoren für Unternehmen in puncto Cyberkriminalität. Foto: Szabowski

Doch wer sind diese Kriminellen? Auch auf diese Frage hatte der Experte eine Antwort: „Es sind in 62 Prozent der Fälle ehemalige und aktuelle Mitarbeiter, die sich als Angreifer oder Anstifter herausstellen." Man sollte dennoch jetzt nicht jeden Mitarbeiter verurteilen, gleichzeitig aber nicht völlig blind sein, riet Krause. Diese Angreifer bräuchten gar keine hochprofessionellen Informatiker sein, ausreichen würde etwas Interesse und Zeit. „In der sogenannten Underground Economy (UE), kann man sich alles besorgen, was man braucht: Waffen, Drogen oder aber auch Schadsoftware. Und das alles kann man dann gemütlich in den virtuellen Einkaufswagen packen", zeigte er anhand von ausgewählten Seiten. So könne man bereits für kleine Beträge, etwa fünf Euro, einen Onlineshop für eine Stunde lahmlegen lassen. Als Beispiel nannte er Unternehmen, deren Internetshop für drei Tage nicht aufgerufen werden konnte. Dem Unternehmen entstand daraus ein Schaden in den Hunderttausenden. Die Täter waren zwei Jugendliche, die gerade mal 150 Euro erpressen wollten. „Sie sehen, wie teuer solche Straftaten sein können. Die Strafen für die Täter sind im Vergleich dazu sehr gering", so Krause.

Die zwei häufigsten Angriffe geschehen entweder via sogenannter Ransomware, einem Programm, das Onlineseiten lahmlegt, oder dem „CEO-Fraud". Hierbei handelt es sich um eine Betrugsmasche, bei der Angestellte von angeblichen Geschäftsführern, zumeist unter Verwendung falscher Identitäten, aufgefordert werden, große Geldsummen des Unternehmens auf fremde Konten zu überweisen. „Technisch ist diesen Leuten nicht beizukommen. Die E-Mails, denn nur darüber findet der Kontakt statt, sehen fast wie im Original aus", erläuterte der Experte. Sollte jemandem so etwas auffallen, riet Krause, sich an die Polizei zu wenden. Diese werde dann versuchen, nicht nur Schlimmeres zu verhindern, sondern auch die Täter ausfindig zu machen. Allerdings, das stellte Krause auch klar, sei es bisweilen schwierig, die Kriminellen zu fassen. Deswegen sei es ihm besonders wichtig, bei Unternehmern ein Bewusstsein für diese Probleme zu schaffen.

Andreas Kötter, Leiter der Unternehmenssicherheit der Volksbank Mittelhessen, führte dann aus, welche Maßnahmen sein Institut durchführt, um die Sicherheit der Kunden zu garantieren. „Unser Geschäftsmodell bedarf vieler Informationen von Ihnen. In Zeiten stetig steigender Kommunikation müssen wir Sie schützen", richtete er sich an die Gäste. Damit kein Geldraub stattfinden könne – wie etwa bei der Bank of Bangladesh, wo knapp 81 Millionen Euro durch Cyberkriminelle entwendet wurden –, habe die Volksbank ein spezielles System entwickelt. Dieses basiere auf Prävention, Detektion und Reaktion, erläuterte Kötter. Foto: Szabowski