„Die Frage ist nicht, ob ein Unternehmen von einem Cyberangriff betroffen wird, sondern wann", meint Harald Pickert, Präsident des Bayerischen Landeskriminalamtes.

„Es gibt keinen hundertprozentigen Schutz"

LKA-Präsident Harald Pickert über den Kampf gegen Cybercrime

Der Präsident des Bayerischen Landeskriminalamtes Harald Pickert war am 27. April zu Gast im Zahnärztehaus München. Wir sprachen mit ihm über die Gefahren, die von Cyberkriminellen ausgehen. Eine wichtige Erkenntnis: Auch Zahnarztpraxen sollten aufgrund der immer aggressiver auftretenden Täter ihre Schutzmaßnahmen überprüfen und gegebenenfalls erhöhen.

BZB: Wie bewerten Sie aktuell die Gefährdung der deutschen Wirtschaft und Infrastruktur durch Hackerattacken?
Pickert: Aufgrund der derzeitigen Steigerung der Fallzahlen ist nicht die Frage, ob ein Unternehmen von einem Cyberangriff betroffen wird, sondern wann und ob dieser Sicherheitsvorfall zu einem Schaden führt, beziehungsweise ob es gelingt, die Reichweite der Auswirkungen des Angriffes zu begrenzen und die Chaosphase nach dem Angriff schnell zu überwinden. Vor allem kleine und mittlere Unternehmen werden zunehmend mit solchen Attacken konfrontiert. Dabei steht jedoch meist nicht der gezielte Angriff auf ein Unternehmen im Fokus, sondern eine großflächig angelegte Kampagne, die vor allem auch durch „Crime-as-a-service" nicht viel Aufwand für den Täter bedeutet. Die größte Gefahr im Unternehmenssektor geht nach wie vor von Verschlüsselungssoftware aus.

BZB: Kann man die Zahl der Angriffe messen?
Pickert: Die Anzeigebereitschaft ist im Phänomenbereich Cybercrime relativ gering. Dies führt zu einem sehr großen Dunkelfeld in der Cyberkriminalität. In der polizeilichen Kriminalstatistik (PKS) wurden im Jahr 2021 insgesamt 39 469 Delikte aus dem Bereich Cybercrime im engeren Sinn für Bayern erfasst, darunter rund 380 Ransomware-Fälle.

BZB: Wo sitzen die Hacker?
Pickert: Im Bereich Cybercrime, in dem die Täter aufgrund der Omnipräsenz des Internets nicht an Ländergrenzen gebunden sind und weltweit von jedem Internetanschluss aus agieren können, sind viele sogenannte Auslandsdelikte festzustellen. Viele Täter schädigen bayerische Bürger und Unternehmen aus dem Ausland heraus beziehungsweise der Handlungsort des Täters ist unbekannt. Die Ermittlung der Aufenthaltsorte von Tätern gestaltet sich schwierig, da sie oftmals technisch sehr versiert sind und aktiv

ihre Spuren im Internet verschleiern. Tätergruppierungen sind oft weltweit vernetzt und arbeiten international zusammen, daher ist auch eine globale Kooperation von Ermittlungsbehörden notwendig. Bei der Ermittlung von Hackerangriffen verweisen digitale Spuren immer wieder auf den osteuropäischen Raum, unter anderem werden auch Russland, China und der Iran als Brennpunkte der Aktivität von Hackergruppierungen gesehen.

BZB: Welche Motive spielen bei Hackerattacken eine Rolle?
Pickert: Über die Motive lässt sich häufig nur mutmaßen. Mehrheitlich sind monetäre Ziele als Motiv erkennbar. In letzter Zeit sind aber durchaus auch politische Motive zu verzeichnen, beispielsweise durch die politische Positionierung von bekannten Angreifergruppierungen im Zusammenhang mit der Ukrainekrise.

BZB: Wie können sich Unternehmen und Privatpersonen vor Hackerangriffen schützen?
Pickert: Einen hundertprozentigen Schutz vor Cyberangriffen gibt es nicht. Das Risiko kann jedoch durch die Umsetzung technischer Präventionsmaßnahmen, die Sensibilisierung der Mitarbeiter und die Umsetzung organisatorischer Maßnahmen erheblich reduziert werden.

Die technischen Sicherheitsmaßnahmen sollten durch die eigene qualifizierte IT-Abteilung beziehungsweise durch einen IT-Dienstleister umgesetzt werden. Das menschliche Fehlverhalten stellt aber eines der größten Einfallstore für Cybercrime-Angriffe dar. Die Zahl der Phishing-Angriffe beziehungsweise Social Engineering-Angriffe ist besonders in Zeiten von Corona angestiegen. Daher ist es besonders wichtig, ein Sicherheitsbewusstsein sowohl in technischer Hinsicht, aber insbesondere auch mit Blick auf die soziale Kompetenz zu schaffen. Hierzu sind spezielle IT-Sicherheitsschulungen wie Mitarbeiter-Awareness-Schulungen wirksame Maßnahmen. Organisatorische Maßnahmen sind essenziell, um von einer sicheren IT profitieren zu können. Sie umfassen Abläufe im Unternehmen, um einerseits den sicheren Umgang mit Daten zu gewährleisten und andererseits Handlungssicherheit bei einem IT-Sicherheitsvorfall zu geben. Ein ganzheitliches IT-Sicherheitskonzept kann potenzielle Gefahren minimieren und die essenziellen Unternehmensdaten schützen. Es bietet ferner fest definierte Abläufe zur Bewältigung von IT-Sicherheitsvorfällen.

Privatpersonen können auf unterschiedlichen Wegen Opfer von Hackerangriffen werden. Gerade in privaten Haushalten zieht immer mehr das sogenannte „Smart Home" oder „Smart Living" ein. Intelligente Geräte wie Saugroboter oder Türklingeln lassen sich über das Internet steuern. Gerade der Fernzugriff beispielsweise über eine App ist praktisch und für viele Menschen aus ihrem heutigen Leben nicht mehr wegzudenken. Um all diese Vorteile sicher nutzen zu können, ist es sehr wichtig, sich auch mit dem Schutz auseinanderzusetzen. Aktualisieren Sie regelmäßig die Software Ihrer Geräte und richten Sie ein separates WLAN für diese Geräte auf dem heimischen Router ein, um zwei Beispiele zu nennen.

BZB: Wie gut ist die bayerische Polizei im Kampf gegen Cyberkriminelle aufgestellt?
Pickert: Die bayerische Polizei setzt im Kampf gegen Cyberkriminelle auf mehrere Säulen. Ein Element war der Launch der Hotline für IT-Notfälle, um eine schnellere Kontaktaufnahme für Bürger bei den staatlichen Stellen zu ermöglichen. Durch die Hotline wurde eine unkomplizierte Möglichkeit für Bürgerinnen und Bürger geschaffen, bei Cyberangriffen schnell in Kontakt mit einer sachkundigen Stelle treten zu können. Aufbauend auf den Erkenntnissen der Hotline wurde mit der Konzeptionierung eines virtuellen Assistenten begonnen. Ziel des Chatbots ist die Gewährleistung einer Rund-um-die-Uhr-Verfügbarkeit sowie eine medienbruchfreie Kommunikation mit den Bürgerinnen und Bürgern. Ebenfalls dient der Chatbot zur zeitnahen Zurverfügungstellung von Informationen, um bei aktuellen Cybercrime-Phänomenen adäquat beraten zu können.

Ein weiteres Element ist die Einrichtung von Quick-Reaction-Teams. Bisherige Erfahrungen mit Cybercrime-Angriffen auf bayerische Unternehmen haben gezeigt, dass sich insbesondere Ransomware-Attacken teilweise als existenzielle Bedrohung für den wirtschaftlichen Fortbestand von Unternehmen darstellen. Hieraus ergeben sich für die Polizei besondere Herausforderungen, die regelmäßig über die polizeilichen Standardmaßnahmen zur Gefahrenabwehr und Strafverfolgung hinausgehen. Die Quick-Reaction-Teams gewährleisten eine Rund-um-die-Uhr-Verfügbarkeit. Die wahrzunehmenden Aufgaben untergliedern sich grundsätzlich in die Aufgabenfelder taktische Betreuung/Beratung, Ermittlungen und Digitale Forensik. Zur notwendigen Qualifizierung des Personals hat die Bayerische Polizei seit 2011 die Sonderlaufbahn der IT-Kriminalisten eingeführt. Hierbei werden studierte Informatiker in einer einjährigen polizeifachlichen Unterweisung zu Polizeivollzugsbeamten ausgebildet, um die Dienststellen bei der Bekämpfung der Cyberkriminalität zu unterstützen. Erfahrungswerte aus der polizeilichen Praxis unterstreichen den Mehrwert des Einsatzes der IT-Kriminalisten. Hinzu kommen rund 100 IT-Forensiker, die durch Sicherung und Aufbereitung digitaler Spuren die Ermittlungen unterstützen.

BZB: Wie wichtig ist die internationale Zusammenarbeit bei der Bekämpfung von Cyberkriminalität?
Pickert: Bei der Bekämpfung von Cyberkriminalität ist eine internationale Zusammenarbeit häufig ausnahmslos unabdingbar. Denn Cyberkriminalität kennt keine Landesgrenzen. Die Täter sitzen häufig im Ausland und verschlüsseln nicht nur deutsche Firmen, sondern agieren international. Dazu nutzen Cyberkriminelle unterschiedliche Serverstrukturen, deren Standorte sich meist im außerbayerischen Ausland befinden. Gleiches gilt für die verwendeten Messenger-Dienste und verwendeten E-Mail-Anbieter. Aufgrund Anfragen zu Bestandsdaten im Laufe des Verfahrens sind internationale Kontakte äußerst wichtig, da über den formalen Weg mittels Rechtshilfeersuchen eine zeitnahe Beauskunftung nicht zielführend möglich wäre.

Vielen Dank für das Gespräch!

Die Fragen stellte Leo Hofmeier.