NACHRICHTEN AG

17. August 2024

Cybercrime im Fokus: Ulmer Unternehmen kämpfen gegen digitale Bedrohungen

Erfahren Sie, wie die Polizei im Polizeipräsidium Ulm gegen Cybercrime vorgeht, um Unternehmen vor Ransomware-Angriffen zu schützen.

Cyberangriffe haben sich in den letzten Jahren zu einer der größten Bedrohungen für Unternehmen und die Gesellschaft entwickelt. Eine Studie des Branchenverbands Bitkom zeigt, dass im Jahr 2023 bereits 72 Prozent aller deutschen Unternehmen von Cybercrime betroffen waren. Besonders alarmierend ist die Zahl der Firmen, die angeben, dass diese Angriffe ihre wirtschaftliche Existenz gefährden. Die Gesamtschäden belaufen sich auf stolze 206 Milliarden Euro, wobei ein Großteil, etwa 148 Milliarden Euro, auf Cyberattacken zurückzuführen ist. Bitkom-Präsident Ralf Wintergerst bezeichnete diese Entwicklungen als die derzeit größte Bedrohung für Wirtschaft, Gesellschaft und Staat.

Die Herausforderungen der Betroffenen

Unternehmen im Zuständigkeitsbereich des Polizeipräsidiums Ulm, das auch die Landkreise Alb-Donau, Biberach, Göppingen und Heidenheim umfasst, sind ebenfalls nicht vor solchen Angriffen gefeit. Ralf Möschen, Leiter der Kriminalinspektion 5, erklärt, dass pro Monat mindestens ein größerer Ransomware-Angriff gemeldet wird. Diese Angriffe betreffen sowohl kleine Handwerksbetriebe als auch große Unternehmen. Trotz der weit verbreiteten Gefahr zögern viele Firmen, nach einem Cyberangriff die Polizei zu alarmieren, aus Angst vor einem

möglichen Imageverlust oder dem Glauben, dass die Polizei nicht über das notwendige Know-how verfüge, um solche Fälle effizient zu bearbeiten.

Ursachen und Einfallstore

Cyberkriminalität reicht von Phishing-Mails, bei denen Benutzer dazu verleitet werden, schädliche Links zu klickenden, bis hin zu gezielten Sabotageakten von staatlichen Akteuren. Möschen spricht von offenen Sicherheitslücken, die von Tätern ausgenutzt werden, sowie von „Zero-Day-Exploits“, d.h. Schwachstellen, für die noch keine Sicherheitsupdates existieren. Ransomware-Angriffe sind dabei sehr lukrativ für die Täter, die üblicherweise Lösegelder in Höhe von drei Prozent des Jahresumsatzes fordern, oft in Kryptowährung wie Bitcoin.

So schützen sich Unternehmen und Privatpersonen

Die Frage, wie sich Unternehmen und Privatpersonen effektiv schützen können, stellt sich in diesem Kontext zwangsläufig. Ralf Möschen und seine Kollegen aus der Kriminalinspektion empfehlen eine erhöhte Wachsamkeit. Besonders wichtig sei, das persönliche Misstrauen zu schärfen, insbesondere bei E-Mails, die nach sensiblen Informationen fragen. Sichere Passwörter sowie Zwei-Faktoren-Authentifizierungen stellen einen ersten Schutz dar. Jedoch ist es auch entscheidend, dass Unternehmen ein umfassendes Sicherheitskonzept implementieren.

Schwierigkeiten bei der Täterermittlung

Wenn es zu einem Angriff kommt, ist die Ermittlungsarbeit der Polizei vielschichtig. Die Ermittler müssen herausfinden, wie die Angreifer in das Unternehmensnetzwerk gelangten, wie lange sie aktiv waren und ob Daten gestohlen wurden. Doch der Weg zum Täter ist oft schwierig, da die Kriminalität gut organisiert ist

und die Täter im Darknet kommunizieren. Möschen hebt hervor, wie international vernetzt und flexibel die Cyberkriminellen sind und dass die Polizei häufig auf internationale Rechtshilfe angewiesen ist. Trotz dieser Herausforderungen wird die internationale Zusammenarbeit immer besser, nicht zuletzt durch die erweiterte Wahrnehmung der Gefahren durch Cyberkriminalität.

Fazit: Cybercrime – ein ernstes Risiko für alle

Abschließend lässt sich feststellen, dass Cyberangriffe nicht nur ein technisches Problem sind, sondern auch tiefere gesellschaftliche und wirtschaftliche Auswirkungen haben. Viele Unternehmen sind sich der wachsenden Gefahr, die solche Angriffe darstellen, nicht bewusst. Es ist vielmehr eine Frage des ‚Wann' es zu einem Angriff kommen könnte, nicht ‚Ob'. Deshalb ist es unabdingbar, präventive Maßnahmen zu ergreifen, um sich bestmöglich auf zukünftige Cyberbedrohungen vorzubereiten.

Details