Beitrag des Landeskriminalamts Berlin - LKA 724 (ZAC) zum Sondernewsletter der IHK zum Thema Cybersicherheit

Die Bedrohungen für IT-Infrastrukturen und Organisationen durch Cyberangriffe entwickeln sich sowohl in der Quantität aber auch in der Qualität und Komplexität stetig weiter. Ansteigend sind auch die von uns zu beobachtenden Ausfallzeiten der Firmen-IT, bevor diese wieder funktioniert. Zeiträume von mehreren Monaten nach einem Ransomware-Befall sind dabei keine Seltenheit!

Um den Schaden bei einem IT-Sicherheitsvorfall möglichst gering zu halten, ist es unabdingbar, sich adäquat vorzubereiten. Hier sind gar nicht so sehr rein technische Vorkehrungen gemeint, sondern auch ein ganzheitliches Konzept für ein Notfallmanagement. Darunter fallen angepasste **Prävention,** die **Detektion** von Gefährdungen und die **Reaktion** auf IT-Sicherheitsvorfälle.

Prävention umfasst dabei Thematiken wie IT-Grundschutz, Konzeptionierungen und Geschäftsprozesse für sichere IT-Umgebungen, aber auch konkret die Vorbereitung auf IT-Sicherheitsvorfälle.

Im Rahmen der Prävention kann durch die Zentrale Ansprechstelle Cybercrime (ZAC) im LKA 724 der Polizei Berlin viel erprobte Unterstützung im Sinne von Awareness, Aufklärung zu Gefahrenpotenzialen und aktuellen Bedrohungen sowie Hinweise und Vorbereitung zu Abläufen speziell bei IT-Sicherheitsvorfällen erfolgen. Idealerweise helfen Veranstaltungen im Rahmen der Prävention dann mindestens dabei, im Krisenfall angemessen schnell und zielgerichtet reagieren zu können. Hier können sehr grundlegende und wenig exponierte Geschäftsprozesse im Ernstfall über den Erfolg oder Misserfolg von geeigneten Gegenmaßnahmen entscheiden.

Die Detektion von Cyberangriffen bzw. IT-Sicherheitsvorfällen ist in modernen, häufig komplexen IT-Infrastrukturen, aber auch in ausgelagerten, schlanken IT-Bereichen eine Kunst für sich. Durch die konkrete Ermittlungserfahrung und Unterstützung in der Bewältigung von Cyberangriffen kann hier durch die ZAC der Polizei Berlin verschiedentlich unterstützt werden. So werden regelmäßig Warnmeldungen bis hin zu konkreten Auffälligkeiten in IT-Netzwerken oder verteilten Systemen und deren Software bekannt und an betroffene Organisationen kommuniziert. Auch in laufenden Ermittlungen bieten die Erkenntnisse nachgelagerter Experten, wie dem Bundeskriminalamt, dem Bundesamt für Sicherheit in der Informationstechnik und Europol ebenso Unterstützung, nicht nur zur Namhaftmachung der Täter, sondern vielmehr (zunächst) gefahrenabwehrend bezüglich der Klärung von Dimension oder weiterem Vorgehen anlässlich eines IT-Sicherheitsvorfalls.

Kritisch ist letztlich die Reaktion auf einen erkannten Cyberangriff bzw. dann das Umsetzen der präventiv erarbeiteten, möglichst ganzheitlichen Maßnahmen im Krisenmanagement. Dabei sind vielzählige Belange und Interessen der Betroffenen gleichzeitig und in häufig

ungewohnter Priorisierung wichtig. Im derzeit stets drohenden Ernstfall eines Cyberangriffs mit Verschlüsselungssoftware und möglichen Datenabflusses spielen dabei rechtliche Fragen (Stichwort: Haftung), aber auch drängende Entscheidungen zur Bewältigung der Lage eine große Rolle. Die ZAC bzw. Ermittler der Polizei Berlin ersetzen dabei kein eigenes Krisenmanagement oder juristische bzw. technische Expertise. Der besondere und geschärfte Blick, mit dem Fokus auf die Aktivitäten cyberkrimineller Gruppen und deren Herangehensweisen, ist allerdings nicht zu unterschätzen.

Insbesondere die Sensibilisierung sowie Unterstützung von Mitarbeitenden als oftmals erste und letzte „Verteidigungslinie“ stehen hier mehr und mehr im Fokus. Denn sowohl das Erkennen als auch das Verhindern eines IT-Sicherheitsvorfalls durch schnelles adäquates Reagieren setzt hier an. Technische Schutzmaßnahmen und ausgeklügelte Datensicherungskonzepte sind unabdingbar notwendig, auch wenn sie im Ernstfall nutzlos werden können; nämlich dann, wenn sensible Daten durch Täter ausgelesen werden konnten. Um diese weitere Dimension eines IT-Sicherheitsvorfalls zu bekämpfen, muss schnell und zielgerichtet reagiert werden.

Wenngleich Cyberkriminelle gern den Eindruck erwecken, durch ausgeklügeltes Hacking nahezu problemlos die Gewalt über IT-Systeme erlangt zu haben, so spielt dieses Szenario zunehmend eine, zumindest statistisch, untergeordnete Rolle. Sicherlich sind adäquate IT-Sicherheitsmaßnahmen so wichtig wie nie, aber sie sichern allerdings auch nur die Teilnahme an einem steten Wettrennen mit den Angriffsmechanismen der international organisierten Täter im Bereich Cybercrime. Der sogenannte **Faktor Mensch**, also das Einwirken auf Mitarbeiter oder Kommunikationsteilnehmer ist in komplexen IT-Infrastrukturen zunehmend von Interesse, um Sicherheitsmaßnahmen aller Art zu überwinden. Mit etwa durch Phishing oder Identitätstäuschung erlangten Nutzer- oder Zugriffsrechten können kritische IT-Systeme, ohne stereotypischen Angriff von außen und mit teils verheerender Wirkung, geführt werden. Letztlich müssen insbesondere die Mitarbeitenden geschützt werden, indem Rechtehierarchien und organisatorische Maßnahmen die Möglichkeiten von Fremdeinwirkung eindämmen und rechtzeitig erkannt werden können.

Bitte sorgen Sie also dafür, dass Ihre Mitarbeitenden wiederholt, aber kreativ sensibilisiert bleiben, im Ernstfall reagieren können und dies durch ein entsprechendes Klima auch frei von Furcht tun!

Autoren: Kriminalhauptkommissar Borries und Kriminaloberkommissar Huwald
Polizei Berlin, Landeskriminalamt – LKA 724 (ZAC)
Senatsverwaltung für Inneres, Digitalisierung und Sport
Abteilung III – Öffentliche Sicherheit und Ordnung
AG Cybersicherheit

Dezember 2022