Heiße Ware

Gesundheitswesen gerät verstärkt ins Visier von Cyberkriminellen

Einrichtungen des Gesundheitswesens geraten verstärkt ins Visier internationaler Hackerbanden. Auch Zahnarztpraxen sind bedroht. Ransomware ist und bleibt die größte Bedrohung, warnt das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem aktuellen Report zur IT-Sicherheit in Deutschland. Einmal eingeschleust, werden Systeme blockiert und häufig auch Personendaten abgegriffen, um Lösegeld zu erpressen. Die Bedrohung im Cyberraum ist so hoch wie nie zuvor.

Zwar ist Deutschland (noch) nicht so gefährdet wie Länder, deren Gesundheitssysteme stärker zentralisiert und digitalisiert sind. So kam es in den USA, Australien, Singapur und Schweden zu schwerwiegenden Angriffen. Die Daten von Millionen Versicherten waren im Netz einsehbar. Aber auch hierzulande häufen sich die Einschläge, obwohl die Daten der Versicherten noch nicht zentral gespeichert werden. Im Mai waren mehr als 30 Krankenkassen von einer Cyberattacke betroffen. Sie waren allesamt Kunden beim IT-Dienstleister Bitmarck. Dieser versicherte zwar, dass keine Patientendaten abgegriffen worden seien. Doch Anwendungen wie die elektronische Patientenakte (ePA) und die eAU waren sehr wohl betroffen, die Kassen waren tagelang nicht per E-Mail erreichbar. Kurz darauf traf es mit der BARMER eine der größten deutschen Krankenkassen. Persönliche Daten von Bonusprogrammkunden flossen nach einem Hackerangriff auf deren IT-Dienstleister ab.

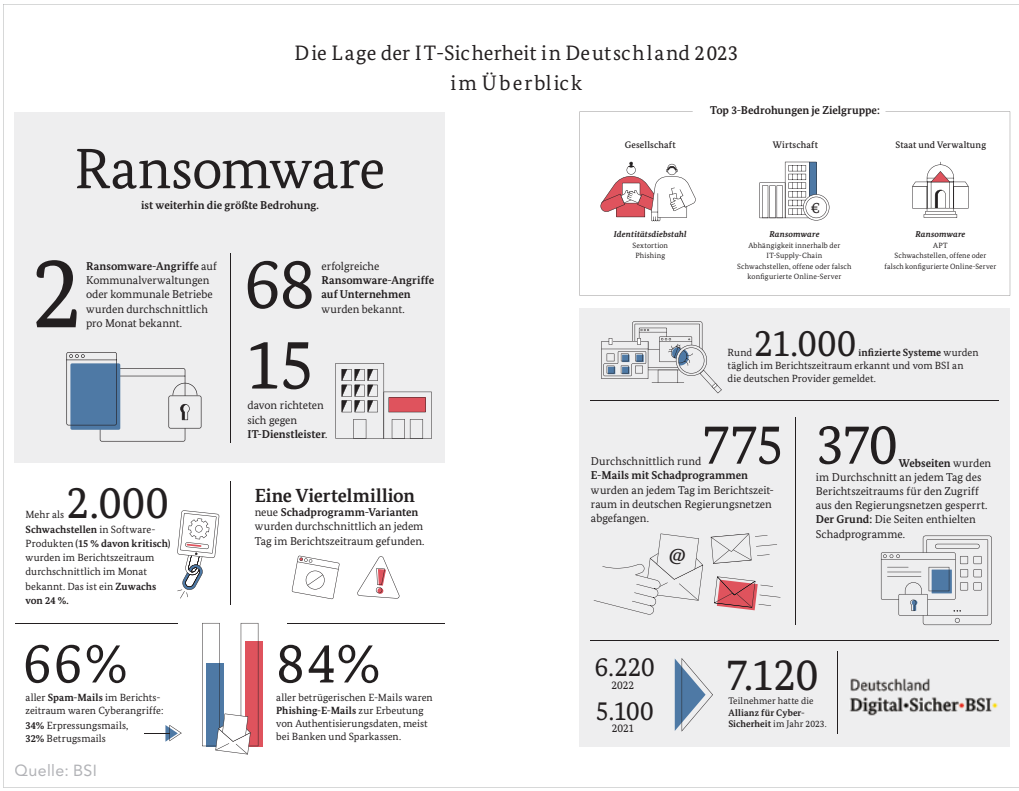
Verlagerung der Attacken

Das BSI beobachtet aktuell eine Verlagerung der Attacken. Nicht mehr nur große, zahlungskräftige Unternehmen stehen im Mittelpunkt, sondern zunehmend auch kleine und mittlere Organisationen sowie staatliche Institutionen, Kommunen und ganz besonders eben Einrichtungen des Gesundheitswesens. Sicherheitslücken in den Systemen treten immer wieder auf und so bleibt die Cybersicherheitslage in Deutschland weiterhin angespannt. Cyberkriminelle werden zunehmend professioneller, sie agieren auch sehr häufig in internationalen Netzwerken. Die Spezialisierung auf bestimmte Dienstleistungen ermögliche es ihnen, ihre „Services“ gezielt zu entwickeln und einzusetzen, so das BSI auf seiner Website. „Wir ordnen die aktuelle Cybersicherheitslage als besorgniserregend ein“, zitiert das „Ärzte-

blatt“ BSI-Präsidentin Claudia Plattner bei der Vorstellung des Reportes Anfang November in Berlin. Laut dem Branchenverband Bitkom betrage der Schaden, der der Volkswirtschaft durch Cyberkriminalität entstehe, im Jahr 206 Milliarden Euro. Ein stolzer Betrag, wenn man den Bundeshaushalt mit 476 Milliarden Euro dagegenhält. Das BSI hatte für seinen Report täglich rund 250 000 neue Varianten von Schadprogrammen und 21 000 mit Schadsoftware infizierte Systeme ermittelt. Hinzu kämen durchschnittlich 70 neue Sicherheitslücken pro Tag, von denen jede zweite als hoch oder kritisch eingestuft werde. Dies entspräche einer Steigerung von 24 Prozent gegenüber dem Vorjahr.

Ransomware ist nach den Erkenntnissen des BSI der häufigste Verursacher. Die dadurch entstehenden wirtschaftlichen Schäden seien enorm. Aber auch sogenannte Supply-Chain-Attacken, bei denen eben nicht die Unternehmen oder Einrichtungen selbst, sondern von ihnen beauftragte Serviceunternehmen ins Visier geraten, nehmen immer mehr zu. Dazu die BSI-Präsidentin: „Wir dürfen uns angesichts der besorgniserregenden Bedrohungslage nicht im Klein-Klein verlieren: Deutschland muss sich als Cybernation verstehen und diesem Selbstverständnis auch Taten folgen lassen.“ Und Bundesinnenministerin Nancy Faeser sprach bei der Präsentation des Berichtes von einer „Zeitenwende“, die eine „strategische Neuaufstellung“ aller verfügbaren Ressourcen erfordere. „Es braucht den intensiven Austausch von Informationen und koordiniertes Handeln, um Bedrohungen aus dem Cyberraum erfolgreich zu begegnen.“ Die institutionelle Zusammenarbeit zwischen Bund und Ländern müsse noch besser werden.

„Es gibt keinen hundertprozentigen Schutz“, betonte auch der Präsident des Bayerischen Landeskriminalamtes Harald Pickert in einem BZB-Interview (5/2022). Es gehe nicht mehr darum, ob ein Unternehmen von einem Cyberangriff betroffen sein könnte, sondern wann. Und vor allem gehe es auch darum, in welchem Maße der Sicherheitsvorfall Schaden anrichten könne oder ob es schon im Vorfeld gelingen könnte, die Reichweite einzudämmen und die Chaosphase möglichst schnell zu überwinden. Technische Präventionsmaßnahmen, eine Sensibilisierung der Mitarbeiter für derartige Bedrohungen und das Umsetzen organisatorischer Maßnahmen seien an dieser Stelle das A und O.



Desinformation durch KI

Die Professionalität, mit der Angreifer im Cyberraum vorgehen, zeigt sich mittlerweile auch im gezielten Einsatz von künstlicher Intelligenz (KI) und deren vielfältigen Werkzeugen, mit denen Texte, Stimmen oder Bildmaterial geschaffen, verändert oder verfälscht werden können. Desinformation und Cybermobbing durch gefälschte Bilder oder Videos sind also neu auftretende Gefährdungen, mit denen sich Unternehmen und Einrichtungen zunehmend konfrontiert sehen werden.

ePA lockt Hacker an

Noch attraktiver für internationale Hackerbanden dürfte das deutsche Gesundheitssystem dann werden, wenn die elektronische Patientenakte flächendeckend eingeführt wird. Datenschützer bemängeln seit Langem, dass Fragen des Datenschutzes ungeklärt seien. Die stellvertretende KZVB-Vorsitzende Dr. Marion Teichmann stellte im BZB 3/2023 klar, dass für Sicherheitslücken, die durch die Telematik-Infrastruktur entstehen, nicht die Praxisinhaber verantwortlich gemacht werden dürfen. „Niemand von uns hat sich freiwillig den Konnektor in die Praxis gestellt. Wir werde vom Gesetzgeber dazu gezwungen, permanent online zu sein. Da ist es nur logisch, dass man uns von jeder Haftung entbindet. Für die Folgen eines Hackerangriffs müssen entweder die PVS-Hersteller oder der Gesetzgeber aufkommen“, so Teichmann.

Ingrid Scholz
Leo Hofmeier