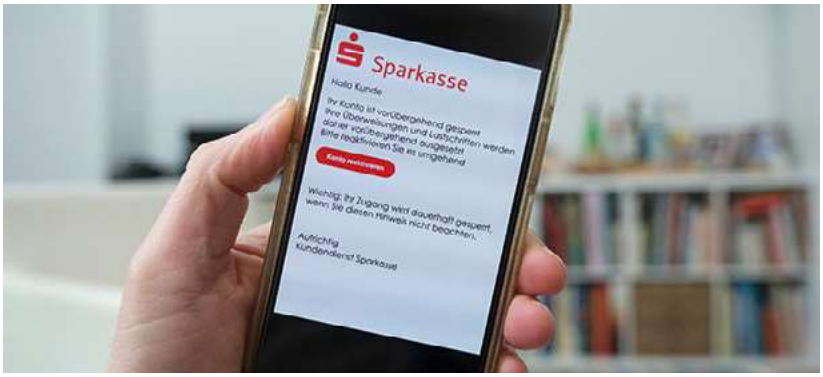
Cyberkriminalität 2023: Enormer gesamtwirtschaftlicher Schaden und hohe Dunkelziffer

Im Bundeslagebild Cybercrime 2023 des Bundeskriminalamts (BKA) liegen Straftaten im Bereich Cybercrime in Deutschland weiter auf einem hohen Niveau. Dabei entsprächen die Zahlen bei weitem nicht den tatsächlichen Fällen, von denen viele den Behörden erst gar nicht bekannt werden.



© IMAGO / Guido Schiefer

Achtung Phishing: Cyberangriffe zielen häufig darauf, vertrauliche Daten von Bankkunden abzugreifen.

Einer Auswertung des BKA und der Landeskriminalämter zufolge haben im Jahr 2023 bundesweit mehr als 800 Unternehmen und Institutionen Ransomware-Fälle bei der Polizei zur Anzeige gebracht. Gleichzeitig gehen die Behörden von einer hohen Dunkelziffer aus. Anlässlich der Deutschen Compliance Konferenz in Düsseldorf im Juni 2024 sagte auch Markus Hartmann, Leitender Oberstaatsanwalt, Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen – ZAC NRW –, Generalstaatsanwaltschaft Köln: „Die Zahlen, die Sie im Cyber-Crime-Bericht sehen, sind ein Bruchteil dessen, was tatsächlich existiert." In bestimmten Deliktskategorien der digitalen Kriminalität würden 90 Prozent der Fälle den Behörden erst gar nicht bekannt werden.

Den enormen gesamtwirtschaftlichen Schaden der Cyberangriffe beziffert der Verband Bitkom für das Jahr 2023 mit 148 Mrd. Euro erneut auf sehr hohem Niveau.

Insbesondere die Anzahl der Cyberstraftaten, die zu Schäden in Deutschland führen, jedoch aus dem Ausland oder von einem unbekannten Ort aus verübt werden, steigt seit ihrer Erfassung im Jahr 2020 kontinuierlich an – 2023 um 28 % gegenüber dem Vorjahr. Wie das BKA mitteilt, übersteigt die Zahl der Auslandstaten im Phänomenbereich Cybercrime damit erneut die der Inlandstaten, also jener Cyberstraftaten, bei denen Deutschland gleichermaßen Handlungs- und Schadensort ist. Die Inlandstaten stagnieren auf hohem Niveau (134.407 Fälle bzw. -1,8 % gegenüber 2022).

2023 seien den Sicherheitsbehörden aber auch zahlreiche Ermittlungserfolge in Deutschland gelungen, die sich primär gegen die Infrastruktur der Tätergruppierungen richteten. Unter anderem wurden die Plattform „Chipmixer", die größte Geldwäsche-Plattform im Darknet, und mehrere kriminelle Marktplätze wie zum Beispiel „Kingdom Market" abgeschaltet. Wie das BKA mitteilt, konnten zudem Erpressungsaktivitäten mehrerer Ransomware-Gruppierungen gestoppt werden. Außerdem wurde mit „Qakbot" ein gefährliches Schadsoftware-Netzwerk zerschlagen. „Qakbot" kontrollierte über 700.000 infizierte Systeme im Internet, die für kriminelle Zwecke wie die Erpressung von Lösegeldzahlungen mittels Ransomware genutzt wurden. Gerade im Bereich der Cyberkriminalität sei die Zerschlagung solcher Infrastrukturen, die weltweit für kriminelle Zwecke angeboten werden, ein entscheidender Faktor der Kriminalitätsbekämpfung.

Im Fokus der Cyber-Angriffe stand im Jahr 2023 verstärkt das Finanzwesen, wo es gehäuft durch pro-russische Hacktivisten zu DDoS-Angriffen kam, also Angriffe, die zur Überlastung einer Webseite führen. Außerdem waren Phishing-Attacken, mit dem Ziel, Zugangsdaten zu Online-Konten zu erlangen, weiterhin eine beliebte Angriffsmethode. Aber auch Cyberangriffe auf IT-Dienstleister führten zu weitreichenden Folgen in der Finanzbranche: So kam es durch eine Schwachstellenausnutzung in der Software eines IT-Dienstleister Mitte des Jahres zu einer Vielzahl von nachgelagerten Angriffen auf große deutsche Banken und Versicherungen. Unter anderem wurden bei den betroffenen Banken vertrauliche Kundendaten entwendet, die später im Darknet veröffentlicht wurden.

Stets mit einem großen Schadenspotenzial verbunden waren auch Angriffe auf Einrichtungen im Gesundheitswesen. So seien im Dezember 2023 infolge eines Ransomeware-Angriffs auf eine Hospitalvereinigung in mehreren Krankenhäusern die Arbeiten auf den Intensivstationen und in den Radiologie-Abteilungen eingeschränkt. *chk*

Das Bundeslagebild Cybercrime

wird durch das BKA in Erfüllung seiner Zentralstellenfunktion erstellt. Es enthält die aktuellen Erkenntnisse und Entwicklungen im Bereich der Cyberkriminalität in Deutschland und bildet insbesondere die diesbezüglichen Ergebnisse polizeilicher Strafverfolgungsaktivitäten ab. Schwerpunkt des Bundeslagebildes Cybercrime sind die Delikte, die sich gegen das Internet und informationstechnische Systeme richten, die sogenannten Cybercrime im engeren Sinne (CCieS). Delikte, die lediglich unter Nutzung von Informationstechnik begangen werden und bei denen das Internet vorwiegend Tatmittel ist, werden als Cybercrime im weiteren Sinne, CCiwS, bezeichnet. Diese werden daher nicht der CCieS zugeordnet und bleiben bei den Betrachtungen im Bundeslagebild Cybercrime weitestgehend unberücksichtigt.

IMPRESSUM
Verlag
Deutscher Fachverlag GmbH, Mainzer Landstraße 251, 60326 Frankfurt am Main
Registergericht AG Frankfurt am Main HRB 8501
USt-IdNr. DE 114139662
Geschäftsführung: Peter Esser (Sprecher), Sönke Reimers (Sprecher), Thomas Berner, Markus Gotta
Aufsichtsrat: Andreas Lorch, Catrin Lorch, Dr. Edith Baumann-Lorch, Peter Ruß
Redaktion: Christina Kahlen-Pappas (verantwortlich),
Telefon: 069 7595-1153, E-Mail: christina.kahlen-pappas@dfv.de
Verlagsleitung: RA Torsten Kutschke,
Telefon: 069 7595-1151, E-Mail: torsten.kutschke@dfv.de
Anzeigen: Matthias Betzler,
Telefon: 069 7595-2785, E-Mail: Matthias.Betzler@dfv.de
Fachbeirat: Gregor Barendregt, Carl Zeiss AG; Andrea Berneis, Berneis Legal & Compliance; Ralf Brandt, LTS Lohmann Therapie-Systeme AG / Drug Delivery Systems Beteiligungs GmbH; Joern-Ulrich Fink, Central Compliance Germany, Deutsche Bank AG; James H. Freis, Jr., Chief Compliance Officer, Deutsche Börse AG; Otto Geiß, Fraport AG; Mirko Haase, Hilti Corporation; Dr. Katharina Hastenrath, Frankfurt School of Finance & Management; Corina Käsler, Head of Compliance, State Street Bank International GmbH; Olaf Kirchhoff, Schenker AG; Torsten Krumbach, msg Systems AG; Dr. Karsten Leffrang, Getrag; Prof. Dr. Bartosz Makowicz, Europa-Universität Viadrina Frankfurt/Oder; Thomas Muth, Muth-zur-Entwicklung; Stephan Niermann; Dr. Dietmar Prechtel, Osram GmbH; Dr. Alexander von Reden, BSH Hausgeräte GmbH; Hartmut T. Renz, Citi Chief Country Compliance Officer, Managing Director, Citigroup Global Markets Europe AG; Dr. Barbara Roth, Chief Compliance Officer, UniCredit Bank AG; Jörg Siegmund, Getzner Textil AG; Eric S. Soong, Group Head Compliance & Corporate Security, Schaeffler Technologies AG & Co. KG; Elena Späth, AXA Assistance Deutschland GmbH; Dr. Martin Walter, selbstständiger Autor, Berater und Referent für Compliance-Themen; Heiko Wendel, Rolls-Royce Power Systems AG; Dietmar Will, Audi AG.
Jahresabonnement: kostenlos
Erscheinungsweise: monatlich (10 Ausgaben pro Jahr)
Layout: Uta Struhalla-Kautz, SK-Grafik, www.sk-grafik.de