Leseprobe

POLIZEI
DEIN PARTNER
Gewerkschaft der Polizei

Cybercrime

Digitaler Angriff auf die Wirtschaft

Leseprobe

www.vdp-polizei.de

Cybercrime

POLIZEI
DEIN PARTNER
Gewerkschaft der Polizei

Impressum

Verantwortlich für den redaktionellen Teil:
pressto GmbH – agentur für medienkommunikation, Köln

Fotos Titel/Innentitel: wicha/stock.adobe.com

Nachdruck des redaktionellen Teils nur nach ausdrücklicher Genehmigung des Herausgebers.

Sämtliche hier veröffentlichte Anzeigen, die im Kundenauftrag für die Drucklegung vom Verlag gestaltet wurden, sind urheberrechtlich geschützt. Nachdruck, Vervielfältigung und elektronische Speicherung ist nur mit Zustimmung des Anzeigenkunden und des Verlages erlaubt. Verstöße hiergegen werden vom Verlag, auch im Auftrag des Anzeigenkunden, unnachsichtig verfolgt.

Der Verlag behält sich die Verwertung der urheberrechtlich geschützten Inhalte dieses Werkes für Zwecke des Text- und Data-Minings nach § 44b UrhG ausdrücklich vor. Jegliche unbefugte Nutzung ist hiermit ausgeschlossen.

VDP VERLAG DEUTSCHE POLIZEILITERATUR GMBH
Anzeigenverwaltung
Ein Unternehmen der Gewerkschaft der Polizei

Forststraße 3 a • 40721 Hilden
Telefon 0211 7104-0 • Telefax 0211 7104-174
av@vdp-polizei.de

Geschäftsführer: Bodo Andrae, Dominik Lehmanns
Anzeigenleiterin: Antje Kleuker

Gestaltung und Layout: Jana Kolfhaus

Anzeigensatz und Druck: Print Media Group GmbH
St.-Reginen-Platz 5 • 59069 Hamm

© 2025 012-2025-019

www.vdp-polizei.de

Vorwort 2

Cybercrime – Angriffe auf Unternehmen 4

Studie zur Internetkriminalität in der Wirtschaft 7

Cyberangriffe frühzeitig erkennen – Erfolgsfaktor Cyber Security Use Cases 8

Einstiegsplan für Notfälle und nachhaltigen Schutz – IT-Sicherheitsstrategien 10

Cyberkriminalität in Deutschland – Die Täter und die Arbeit der Ermittler 12

Wie schütze ich die Daten in meinem Unternehmen? 15

KRITIS-Schutz: Erste Schritte 18

Vertrauen schafft Sicherheit– Die Arbeit der Zentralen Ansprechstelle Cybercrime (ZAC) in Mecklenburg-Vorpommern 20

Mobile Kommunikationsmittel im Visier von Cyberkriminellen 22

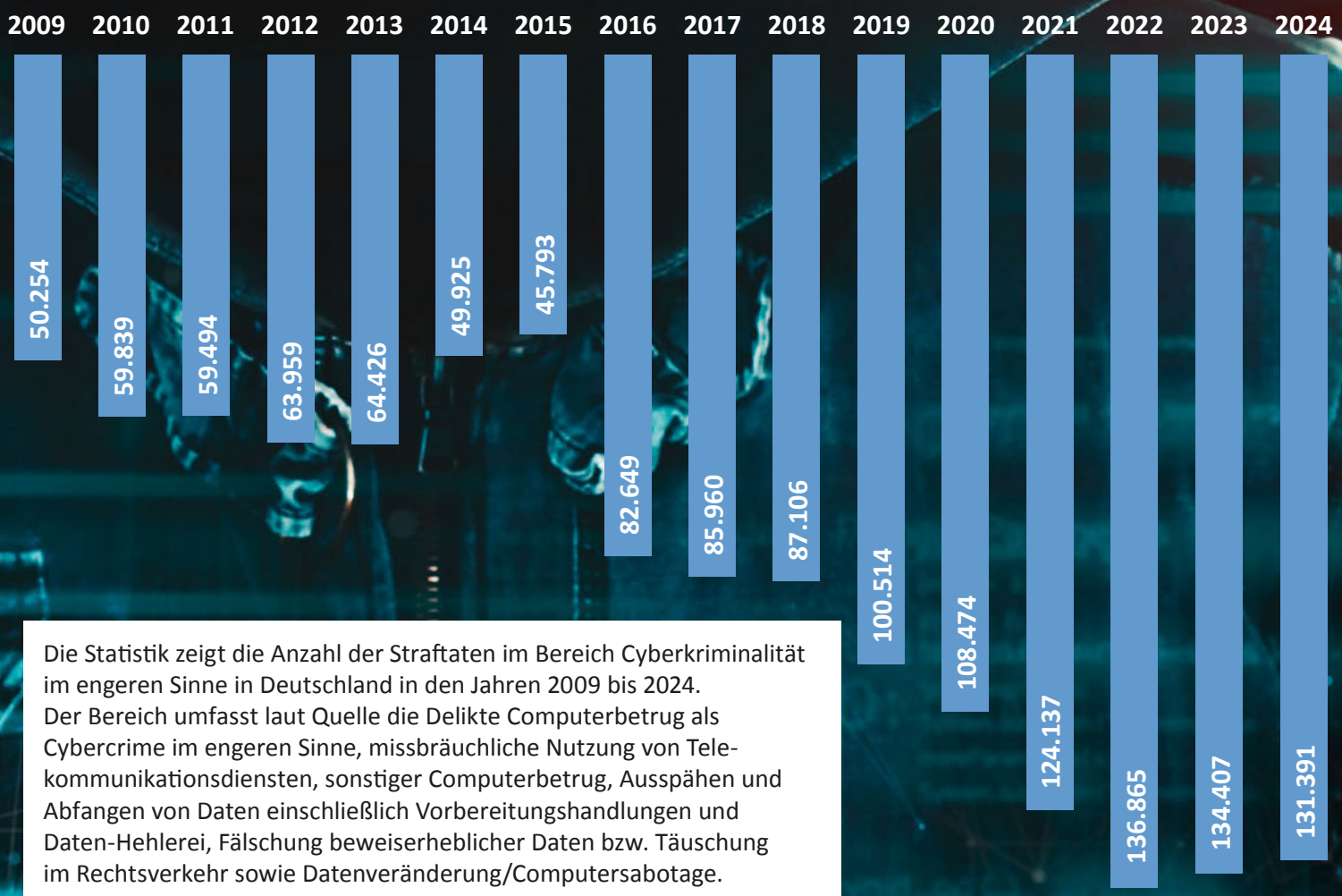
Cloud-Dienste – Pro und Contra 24

Betrug durch KI-gesteuerte Chatbots – Cyberangriffe werden immer persönlicher 26

Probleme mit Cybercrime – Informationsquellen für Unternehmen 28

Präventionspartner der Gewerkschaft der Polizei 28

Polizeilich erfasste Fälle von Cyberkriminalität in Deutschland bis 2024



Die Statistik zeigt die Anzahl der Straftaten im Bereich Cyberkriminalität im engeren Sinne in Deutschland in den Jahren 2009 bis 2024.
Der Bereich umfasst laut Quelle die Delikte Computerbetrug als Cybercrime im engeren Sinne, missbräuchliche Nutzung von Telekommunikationsdiensten, sonstiger Computerbetrug, Ausspähen und Abfangen von Daten einschließlich Vorbereitungshandlungen und Daten-Hehlerei, Fälschung beweiserheblicher Daten bzw. Täuschung im Rechtsverkehr sowie Datenveränderung/Computersabotage.

Quelle: Bundeskriminalamt

Liebe Leserin, lieber Leser,

wer meint, Cyberkriminalität in der Wirtschaft betreffe nur große Konzerne, der irrt: Auch kleine und mittelständische Unternehmen müssen sich Gedanken um die Sicherheit ihrer Systeme machen. Denn Datenverlust, Produktionsausfälle, Klagen wegen des Diebstahls von personenbezogenen Daten oder hohe Lösegeldforderungen können große finanzielle Schäden nach sich ziehen. Häufig wird das Risiko von den Unternehmen jedoch unterschätzt, nach dem Motto: „Bei uns gibt es nichts Interessantes zu holen." Ein Irrglaube, denn insbesondere der deutsche Mittelstand verfügt über enormes Fachwissen und wichtige Patente, die Begehrlichkeiten wecken.

Vor allem so genannte Ransomware-Angriffe haben in den vergangenen Jahren zugenommen. Dabei erpressen die Täter zum Teil hohe Geldsummen von Unternehmen, indem sie zum Beispiel Daten verschlüsseln und mit deren Veröffentlichung drohen. Kriminalhauptkommissar a.D. Peter Vahrenhorst vom Landeskriminalamt Nordrhein-Westfalen erklärt, wie die Täter dabei konkret vorgehen. Wie sich Unternehmen vor solchen und anderen Angriffen aus dem Netz schützen können, verrät Felix Kuhlenkamp, Experte für Cybersicherheit beim Branchenverband Bitkom. Guido Steentjes von der ConSecur GmbH hebt hervor, dass es entscheidend ist, potenzielle Bedrohungen frühzeitig zu erkennen. Er erklärt, wie das mit einem Cyber Security Use Case erreicht werden kann.

Unterstützung bei der konkreten Planung und Umsetzung von IT-Sicherheitsmaßnahmen erhalten Unternehmen zum Beispiel von der „Transferstelle IT-Sicherheit im Mittelstand" (TISiM). Im Heft werden die konkreten Hilfeleistungen vorgestellt.
Aber auch die Polizei unternimmt viel, um in Unternehmen ein Bewusstsein für Cybercrime und IT-Sicherheit zu schaffen. Die „Zentralen Ansprechstellen Cybercrime" (ZAC) der Landeskriminalämter sind etwa kompetente Anlaufstellen für alle Wirtschaftsunternehmen – und das nicht erst bei bereits eingetretenem Schaden. Das Problem: Viele Unternehmen scheuen den Gang zur Polizei aus Angst vor einem Imageschaden oder davor, dass Betriebsabläufe durch die polizeilichen Ermittlungen lange zum Stillstand kommen könnten. Jörg Bruhn, Leiter des Digitalen Service- und Kompetenzzentrums (DiSK) im Landeskriminalamt Mecklenburg-Vorpommern, erklärt, wie die Arbeit der Polizei konkret aussieht und warum sich betroffene Unternehmen unbedingt an die Polizei wenden sollten.

Vernachlässigt werden beim Thema IT-Sicherheit oft mobile Endgeräte wie Smartphones, Laptops oder Tablets, aber auch die Arbeit im Homeoffice. Wir klären über aktuelle Bedrohungen, Sicherheitslücken und wirksame Schutzmaßnahmen für mobile Endgeräte auf. Die wichtigsten Sicherheitsmaßnahmen rund um die Datenspeicherung bei Cloud-Diensten erläutert zudem Christian Ehringfeld von der Gewerkschaft der Polizei.

Eine aufschlussreiche Lektüre wünscht
Ihre Redaktion von PolizeiDeinPartner

Bits and Splits/stock.adobe.com