Leseprobe

POLIZEI
DEIN PARTNER
Gewerkschaft der Polizei



Cybercrime

Digitaler Angriff auf die Wirtschaft

Leseprobe

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.

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: Dominik Lehmanns
Anzeigenleiterin: Antje Kleuker

Gestaltung und Layout: Jana Kolfhaus

Anzeigensatz und Druck: WIRmachenDRUCK GmbH
Mühlbachstraße 7 • 71522 Backnang

© 2026 012-2026-019

vdp-polizei.de

Vorwort 2

Cyberangriffe: Milliardenrisiko für Unternehmen 4

IT-Sicherheit gehört in die Chefetage 7

Claude Mythos – Die nächste Evolutionsstufe der Cybersecurity-KI? 10

Probleme mit Cybercrime – Informationsquellen für Unternehmen 13

Wenn der Angriff mit einem gültigen Login beginnt – Warum Unternehmen Identitäten, Rollen und Zugriffe besser schützen müssen 14

Daten schützen, Betrieb sichern – So bauen Unternehmen eine wirksame Cyberabwehr auf 17

NIS-2 und KRITIS: Diese Pflichten gelten aktuell 20

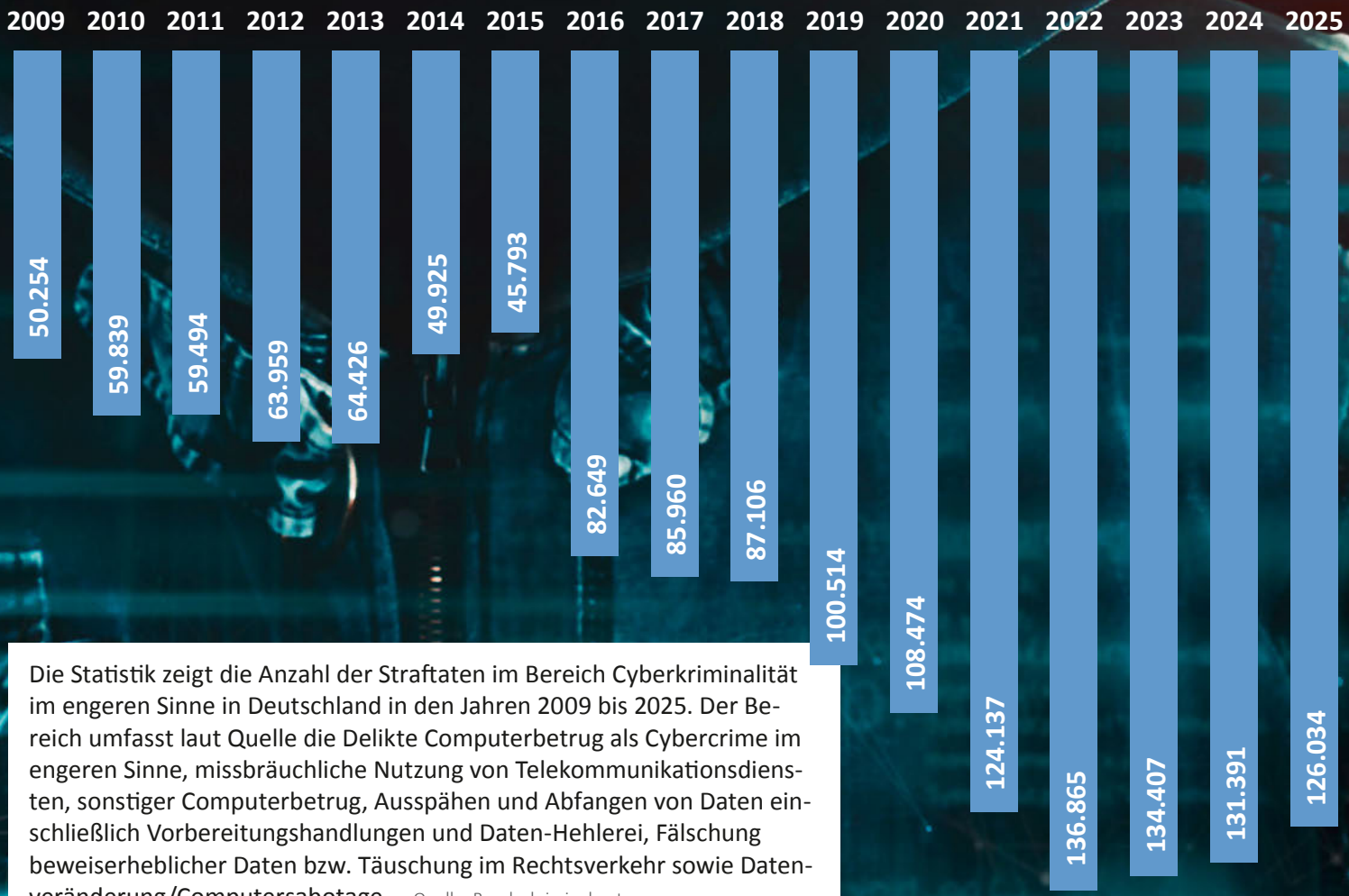
Vertrauen schafft Sicherheit – Die Arbeit der Zentralen Ansprechstelle Cybercrime (ZAC) in Mecklenburg-Vorpommern 22

Organisiert, arbeitsteilig, international – Cyberkriminalität heute 24

Cyberbetrug mit KI: Täuschend echt 26

Präventionspartner der Gewerkschaft der Polizei 28

Polizeilich erfasste Fälle von Cyberkriminalität in Deutschland bis 2025



Die Statistik zeigt die Anzahl der Straftaten im Bereich Cyberkriminalität im engeren Sinne in Deutschland in den Jahren 2009 bis 2025. 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 betreffe vor allem große Konzerne, der irrt: Längst stehen Unternehmen jeder Größe im Visier professioneller Täter. Die wirtschaftlichen Schäden erreichen dabei immer neue Rekordwerte. Datendiebstahl, Erpressung, Produktionsausfälle oder Sabotage können erhebliche finanzielle Folgen haben und im schlimmsten Fall sogar die Existenz eines Unternehmens bedrohen. Gleichzeitig werden die Angriffe immer professioneller, arbeitsteiliger und internationaler.

Vor allem sogenannte Ransomware-Angriffe zählen zu den größten Bedrohungen. Dabei verschlüsseln Kriminelle Daten und Systeme, um Lösegeld zu erpressen. Hinzu kommen Phishing-Angriffe, Passwortdiebstahl und Attacken auf digitale Infrastrukturen. Zunehmend nutzen Täter dabei auch Künstliche Intelligenz, um täuschend echte E-Mails, Stimmen oder Videos zu erzeugen.

Wie sich Cyberkriminalität zu einem professionell organisierten Geschäftsmodell entwickelt hat, erläutert Max Tarantik von der Enginsight GmbH. Er zeigt, warum der Mythos vom Hacker im dunklen Keller längst überholt ist und welche Rolle Arbeitsteilung, Automatisierung und internationale Netzwerke heute spielen. Christoph Kronabel von der ConSecur GmbH wirft einen Blick auf die Zukunft der Cybersicherheit. Am Beispiel der Sicherheits-KI „Claude Mythos“ erklärt er die Chancen und Risiken leistungsfähiger KI-Systeme und zeigt auf, wie Unternehmen sich auf eine neue Generation KI-gestützter Angriffe vorbereiten können.

Dass IT-Sicherheit längst keine reine Aufgabe der IT-Abteilung mehr ist, verdeutlicht ein weiterer Beitrag dieser Ausgabe. Er erläutert, warum Cybersicherheit in die Chefetage gehört und welche Verantwortung Unternehmensleitungen für Risikomanagement, Notfallvorsorge und Compliance tragen. Tim Erkenberg von der unique projects GmbH & Co. KG erklärt zudem, warum moderne Angriffe häufig mit einem scheinbar legitimen Login beginnen und wie Unternehmen Identitäten, Rollen und Zugriffsrechte wirksam schützen können.

Unterstützung bei der konkreten Umsetzung von Sicherheitsmaßnahmen erhalten Unternehmen unter anderem durch die Transferstelle Cybersicherheit im Mittelstand, den CYBERsicher Check und weitere Angebote von Bund und Wirtschaft. Zudem informieren wir über die aktuellen Anforderungen durch die NIS-2-Richtlinie und das KRITIS-Dachgesetz und zeigen, welche Pflichten sich daraus für Unternehmen ergeben.

Aber auch die Polizei engagiert sich intensiv im Kampf gegen Cyberkriminalität. Jörg Bruhn vom Landeskriminalamt Mecklenburg-Vorpommern stellt die Arbeit der Zentralen Ansprechstellen Cybercrime vor und erklärt, wie Unternehmen bereits präventiv unterstützt werden können und warum Betroffene den Kontakt zur Polizei nicht scheuen sollten.

Mithilfe von von Phishing, Deepfakes und intelligenten Chatbots können Kriminelle ihre Angriffe immer glaubwürdiger gestalten – die Schattenseite der Künstlichen Intelligenz. Täuschend echte Stimmen, Bilder und Nachrichten erschweren es, Betrugsversuche zu erkennen und erhöhen die Gefahr für Unternehmen erheblich. Ebenfalls wird erläutert, welche Rolle der AI Act der Europäischen Union spielt, wo die Grenzen der Technologie liegen und wie Unternehmen KI selbst zur Abwehr von Cyberangriffen nutzen können – und zuletzt, wie sie sich wirksam gegen KI-gestützten Betrug schützen können.

Eine aufschlussreiche Lektüre wünscht

Ihre Redaktion von PolizeiDeinPartner

Bits and Splits/stock.adobe.com