6 Der Cybercrime-Markt boomt

Cyberkriminelle nutzen die weltweite Vernetzung zu ihrem Vorteil ...

Die Cybercrime-Industrie hat sich in ein durchorganisiertes, globales Geschäftsmodell entwickelt, dessen Erfolg durch unsere wachsende Abhängigkeit von Technologie genährt wird. Die rasante Zunahme von Remote-Work, vernetzten Geräten und neuen Technologien, wie KI, IoT und Cloud-Umgebungen – das alles hat die Angriffsfläche um ein Vielfaches vergrößert. Cyberkriminelle haben heute mehr mögliche Zutrittstore in unsere Systeme als je zuvor. Jeder Sektor und jede Einzelperson sind heute Teil eines eng verzweigten digitalen Netzes, in dem sich ein einziger Angriff schockwellenartig auf mehrere Unternehmen, Branchen und ganze Gemeinschaften ausbreiten kann. Und das mit verheerenden finanziellen Folgen – **die weltweiten Kosten von Cybercrime sollen dieses Jahr 10 Billionen US-Dollar erreichen**.[1]

Angetrieben wird das Wachstum dieses lukrativen Markts jedoch nicht nur durch seine Größe, sondern vor allem auch durch die ausgeklügelten Methoden der Cyberkriminellen. In Sachen Präzision, Koordination und Anpassungsfähigkeit haben sie ihre Vorgehensweise perfektioniert und zielen oft auf vielversprechende Einzelpersonen oder Organisationen in Rechtssystemen ab, in denen die Nachverfolgung von Cybercrime-Zwischenfällen nicht ausreichend durchgesetzt wird. Für die Koordination ihrer Angriffe über Landesgrenzen hinweg nutzen Cyberkriminelle globale Online-Plattformen wie Telegram, die eine große Reichweite und kaum Einschränkungen bieten. Auch die **Professionalisierung der Cyberkriminalität** durch Dienste wie Ransomware-as-a-Service (RaaS) hat dazu beigetragen, dass der Cybercrime-Markt immer lukrativer wird und die Zutrittsschwelle zur Cyberkriminalität immer weiter sinkt. Aus diesem illegalen Geschäftsmodell hat sich ein breiteres Cybercrime-as-a-Service-Ökosystem entwickelt, das weniger erfahrenen Cyberkriminellen und Neueinsteigern Malware-Kits, Phishing-Templates und Tools für DDoS-Angriffe (Distributed Denial of Service) bereitstellt.[2]

... doch nur durch globale Zusammenarbeit können wir uns den neuen Cyberbedrohungen entgegenstellen

Aktuellen Prognosen zufolge verursachte Cyberkriminalität in Deutschland im Jahr 2024 einen Schaden von 178,6 Milliarden Euro – ein Anstieg von rund 30 Milliarden Euro im Vergleich zum Vorjahr (2023: 148,2 Milliarden Euro).[3] Ohne umgehende Gegenmaßnahmen werden die Zahlen weiter steigen. Isolierte Initiativen sind nicht genug, um uns der wachsenden Bedrohung entgegenzustellen – dazu müssen wir alle an einem Strang ziehen. Durch die Zusammenarbeit über Organisationen, Branchen und Regierungen hinweg können wir Threat Intelligence austauschen, einheitliche Abwehrstrategien entwickeln und die lückenlose Durchsetzung von Richtlinien gewährleisten.

1 **Statista (2024).** Cybercrime Expected to Skyrocket in Coming Years.
2 **Europol (2024).** Cyber-attacks: the apex of crime-as-a-service.
3 **Bitkom (2024).** Angriffe auf die deutsche Wirtschaft nehmen zu.