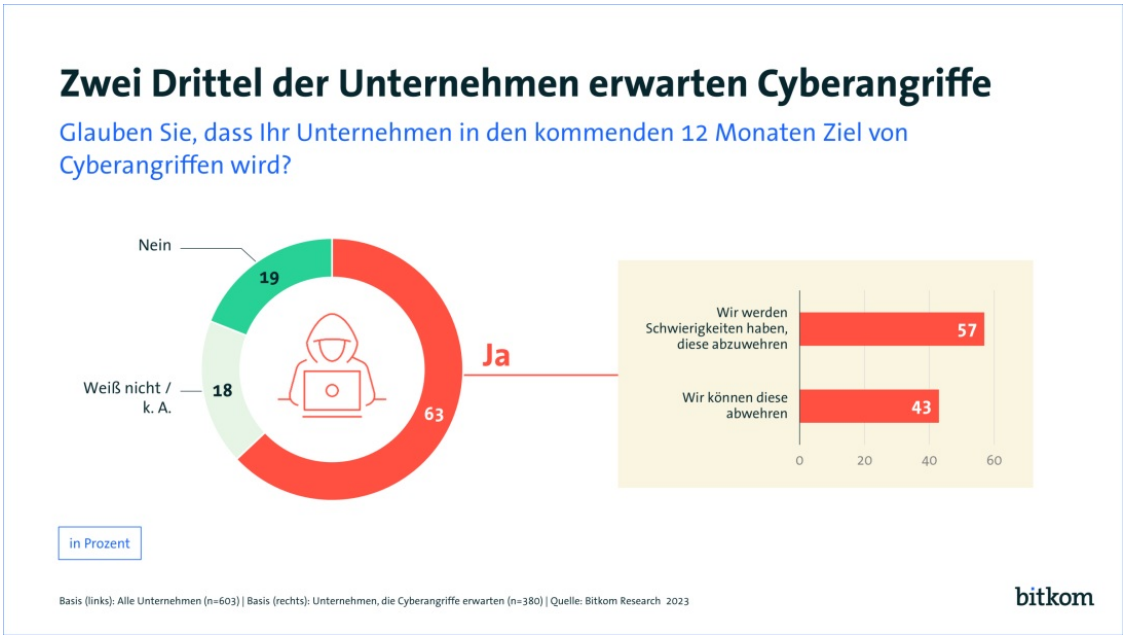
Bitkom e.V. | Presseinformation

# Bitkom und BKA zum Cyberlagebild 2022

**Berlin, 16. August 2023** - Das Bundeskriminalamt (BKA) hat heute sein „Cyberlagebild 2022“ vorgestellt. Auf der gemeinsamen Pressekonferenz mit BKA-Vizepräsidentin Martina Link hat **Bitkom-Präsident Dr. Ralf Wintergerst** dazu erklärt:




„Cyberkriminalität ist eine Bedrohung für unsere Wirtschaft und für unsere Gesellschaft. Sie mag aktuell sogar eine der größten Bedrohungen für Deutschland sein. Und Cyberkriminelle sitzen nicht allein irgendwo in einem Keller, Cybercrime ist längst Teil der weltweiten organisierten Kriminalität und häufig eng mit staatlichen Akteuren uns wenig freundlich gesonnener Länder verknüpft. Eine erfolgreiche Cyberattacke kann die IT eines Unternehmens lahmlegen und damit die gesamte Produktion – und das über Stunden, Tage oder Wochen. Sie kann Krankenhäuser, Infrastrukturen, Energienetze und den Verkehr betreffen. Sie kann als Angriff sichtbar werden und sie kann auch kaum wahrnehmbar Schritt für Schritt über Social Engineering ein Unternehmen infiltrieren. Davon betroffen sind alle Branchen, davon betroffen sind auch die öffentlichen Verwaltungen, Stadtwerke, Energieversorger oder Krankenhäuser.

Wir haben im Vorfeld dieser Pressekonferenz 603 Unternehmen ab 20 Beschäftigten in Deutschland zu ihren Erfahrungen und Einschätzungen rund um Cybercrime befragt.

Fast jedes zweite Unternehmen – 48 Prozent – gibt an, dass ein erfolgreicher Cyberangriff die eigene Existenz bedrohen könnte. Falls jemand meint, das seien übertriebene Befürchtungen: Im Juni musste in Illinois ein Krankenhaus schließen, weil es nach einem Ransomware-Angriff über Monate keine Versicherungsgelder beantragen konnte.

In Deutschland rechnen 63 Prozent der Unternehmen damit, in den kommenden zwölf Monaten Opfer von Cyberangriffen zu werden. Zwei von drei Unternehmen! Man kann sich einen solchen Wert bei „klassischer“ Kriminalität wie Raub oder Erpressung kaum vorstellen. Nur 19 Prozent gehen nicht von einem Angriff aus und 18 Prozent trauen sich keine Einschätzung zu.

Wenn man sich die zwei Drittel der Unternehmen, die einen Angriff erwarten, genauer anschaut, zeigt sich zudem: 43 Prozent von ihnen meinen, den Angriff erfolgreich abwehren zu können. Aber eine Mehrheit von 57 Prozent rechnet mit Schwierigkeiten bei der Abwehr. Was muss also getan werden?

Zum einen sind die Unternehmen selbst gefordert. Nicht einmal die Hälfte der Unternehmen – nämlich 48 Prozent – investiert nach eigener Einschätzung genug in Cybersicherheit. Nur 30 Prozent haben Informationsangebote der Polizei zum Schutz vor Cyberkriminalität genutzt. 41 Prozent räumen sogar ein: Wir haben das Thema Cyberkriminalität bisher verschlafen.

Ich kann nur sagen: Es ist höchste Zeit, aufzuwachen. Wer Verantwortung für ein Unternehmen trägt, muss dafür sorgen, dass IT-Sicherheit nicht allein Thema der IT-Abteilungen ist. IT-Sicherheit gehört ins Top-Management. Und dort sollten drei Dinge ganz oben auf der Agenda stehen.

Erstens: IT-Sicherheit muss mit den notwendigen Ressourcen ausgestattet werden. Dieses Geld ist eine Investition in die Zukunftsfähigkeit des eigenen Unternehmens. Wir empfehlen, nicht weniger als 20 Prozent der gesamten IT-Ausgaben für das Thema IT-Sicherheit bereitzustellen.

Zweitens: Alle Mitarbeiterinnen und Mitarbeiter müssen zum Thema IT-Sicherheit geschult werden. Eines der wichtigsten Einfallstore für Angreifer bleiben die Menschen im Unternehmen – und zugleich bilden sie die erste und vielleicht beste Abwehr bei Angriffen. Solche Schulungen dürfen nicht nur pflichtschuldig einmal durchgeführt werden, sie müssen regelmäßig stattfinden. Denn auch die Methoden und Technologien der Angreifer entwickeln sich weiter.

Und drittens: Jedes Unternehmen braucht einen Notfallplan für Cyberangriffe. Er muss klar regeln, wer im Ernstfall was tut. Wenn ein Unternehmen erst einmal Opfer eines Angriffs wird, ist keine Zeit dafür, sich diese Fragen erstmals zu stellen. Zumal womöglich die unternehmensinterne Kommunikation zunächst nicht mehr funktioniert. Je schneller reagiert wird, desto besser stehen die Chancen, größeren Schaden abzuwenden.

Aber nicht nur die Unternehmen, auch die Behörden sind gefordert. In unserer Umfrage sind 79 Prozent der Unternehmen der Meinung, die Polizei könne international agierende Cyberkriminelle nicht wirksam verfolgen. 74 Prozent meinen, es fehlt in der Polizei an Know-how rund um Cyberkriminalität. Zugleich wollen 78 Prozent, dass die Polizei verstärkt neue Technologien wie KI im Kampf gegen Cyberkriminalität nutzt. 90 Prozent sind dafür, dass die Befugnisse der Polizei im Kampf gegen Cyberkriminelle ausgeweitet werden. Und 91 Prozent fordern, dass die Polizei im Kampf gegen Cyberkriminalität finanziell und personell besser ausgestattet wird.

Die Unternehmen sagen also, es müsse mehr passieren und das ist richtig.  Ganz konkret helfen würde den Unternehmen zum Beispiel ein zentrales, leicht verfügbares und übersichtliches Cyberlagebild. In den vergangenen Jahren ist aber auch schon viel passiert.

Es gibt Zentrale Ansprechstellen für Cybercrime, sogenannte ZAC, in den Landeskriminalämtern. Sie dienen grundsätzlich als Ansprechpartner zum Thema Cybercrime für Unternehmen, Verbände und Behörden. Sie dienen aber auch der Förderung der vertrauensvollen Zusammenarbeit zwischen diesen Akteuren und der Polizei. Allerdings muss man auch sagen, dass die politische Unterstützung der ZACs sehr unterschiedlich ausgeprägt ist.

Wichtig für die Zukunft wird sein, dass wir eine noch stärkere Konzentration von Zuständigkeiten und Know-how hinbekommen. Cyberkriminalität orientiert sich nicht an unseren föderalen Strukturen. Und bei ihrer Bekämpfung erweisen die sich manchmal leider als Hemmschuh. Außerdem gilt: Wir brauchen eine insgesamt höhere Präsenz von Polizei und Strafverfolgungsbehörden im Cyberraum. Die wiederum brauchen dazu Know-how, Personal und technische Ausstattung.

Die Behörden müssen mehr tun. Die Unternehmen müssen mehr tun. Und beide müssen mehr gemeinsam tun.

Bitkom arbeitet deshalb in der Sicherheitskooperation Cybercrime mit den Landeskriminalämtern NRW, Hessen, Baden-Württemberg, Sachsen, Niedersachsen und Rheinland-Pfalz zusammen. Weitere Partner sind natürlich gerne gesehen. Dort geht es um den Austausch über Angriffsmethoden wie Social Identity Fraud oder die Nachverfolgung von Kryptowährungen ebenso wie um Workshops oder Planspiele, um die Reaktion auf einen Cyberangriff zu üben.

Außerdem sind wir in der Allianz für Cybersicherheit aktiv. Mittlerweile umfasst die Allianz ein Netzwerk von über 7.000 Teilnehmern.

Ein Höchstmaß an Cyber-Sicherheit ist entscheidend für die digitale Souveränität und die Wettbewerbsfähigkeit des Innovations-Standorts Deutschland. Jetzt muss es darum gehen, diese

Erkenntnis in Partnerschaft mit den Behörden auch ganz praktisch in ein mehr an Sicherheit umzusetzen.“

## Kontakt

**Andreas Streim**
Pressesprecher
Telefon: +49 30 27576-112
E-Mail: a.streim@bitkom.org
Download Pressefoto

**Felix Kuhlenkamp**
Bereichsleiter Sicherheitspolitik
Download Pressefoto
Nachricht senden

---

Link zur Presseinformation auf der Webseite:
***https://www.bitkom.org/Presse/Presseinformation/Bitkom-und-BKA-zum-Cyberlagebild-2022***