PITS 2024

Informationsaustausch, internationale Zusammenarbeit und Transparenz für mehr Cybersicherheit und Resilienz

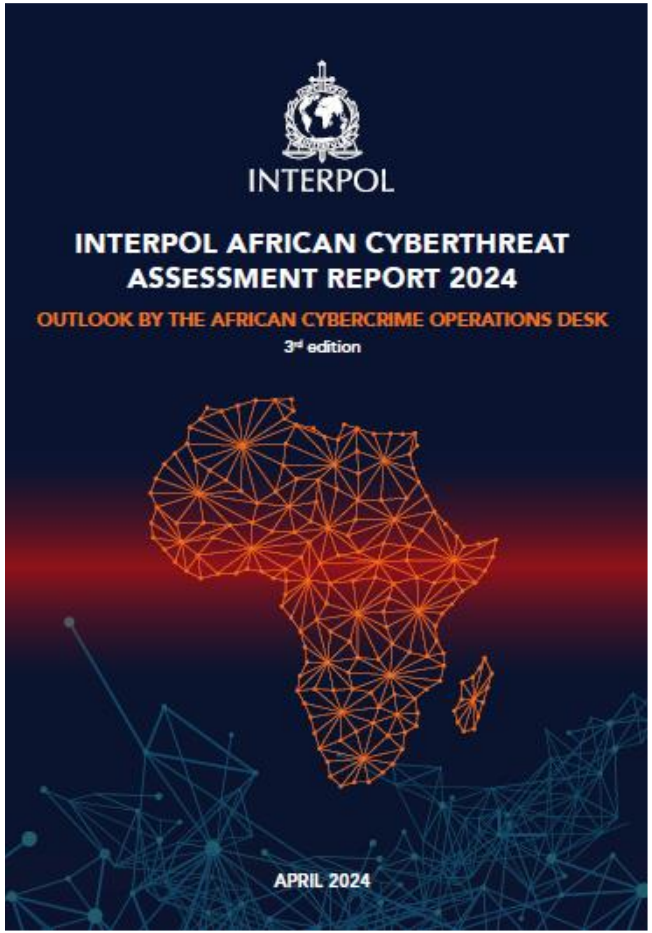
Jochen Michels
Director, Public Affairs, Europe

Eine besorgniserregende Cyber-Bedrohungslage

- Global gab es 2023 im Vergleich zum Vorjahr rund **71 Prozent mehr Opfer von Ransomware**; die Anzahl von Ransomware-Gruppen nahm um 30 Prozent zu. (State of Ransomware Report)
- Kaspersky verzeichneten im Jahr 2023 weltweit rund **33,8 Millionen Angriffe auf mobile Geräte**; das entspricht einem **Plus von fast 52 Prozent** gegenüber dem Vorjahr. In Deutschland wurden 513.441 Angriffe auf Mobilgeräte festgestellt und damit die meisten innerhalb der verglichenen europäischen Länder (Bericht Mobile Bedrohungslandschaft 2023)
- Im Jahr 2023 blockierten die Sicherheitslösungen von Kaspersky in Deutschland auf **18,3 Prozent der industriellen Computer schädliche Objekte**; 2022: 15,1 Prozent. (ICS Threat Landscape Report)
- Im Jahr 2023 gab es rund **34 Millionen Phishing-Angriffe** auf Nutzer in der Bundesrepublik (Spam- und Phishing-Report).

Die wesentliche Basis zur Steigerung von Cybersicherheit und Resilienz sind qualitativ hochwertige Informationen! Deswegen ist der Informationsaustausch über Grenzen und Sektoren hinweg besonders wichtig!

Informationsautausch zur Steigerung von Cybersicherheit und Resilienz



Brasilien und Spanien nutzen die Cyberkapazitäten von INTERPOL, um Ermittlungen miteinander zu verknüpfen

- Brasilien und Spanien führten unabhängige nationale Ermittlungen im Zusammenhang mit der Grandoreiro-Malware durch.
- Auf Bitte beider Länder übernahm die INTERPOL-Einheit für Cyberkriminalität eine koordinierende Rolle, leitete eine Operation ein und zog die Partner Trend Micro, Kaspersky, Group-IB und Scitum hinzu.
- Im Rahmen der Operation konnten fünf Programmierer und Betreiber, die hinter der Banking-Malware standen, verhaftet werden.

Internationale Zusammenarbeit.

Internationale Zusammenarbeit: INTERPOL

- Kooperationsvereinbarung seit 2014
- Schulung, TI, operative Unterstützung
- Im Jahr 2023 hat Kaspersky INTERPOL mit Bedrohungsdaten bei der Operation Africa Cyber Surge II unterstützt
- Die Ermittler waren in der Lage, gefährdete Infrastrukturen zu identifizieren und mutmaßliche Cyberkriminelle in der gesamten afrikanischen Region festzunehmen.
- Die Operation führte zur Verhaftung von 14 Tätern und zur Identifizierung von Netzwerkinfrastrukturen, die mit Schäden von mehr als 40 Millionen Dollar verbunden sind.

INTERPOL

Gründungspartner der No More Ransom Initiative

- Die Initiative ist ein Zusammenschluss von Strafverfolgungsbehörden und IT-Sicherheitsunternehmen zur Bekämpfung von Ransomware-Angriffen und deren Folgen.
- Die Website "No More Ransom" wurde von der National High Tech Crime Unit der niederländischen Polizei, vom Europäischen Zentrum für Cyberkriminalität von Europol, von Kaspersky und McAfee ins Leben gerufen. Sie soll Opfer von Ransomware dabei unterstützen, ihre verschlüsselten Daten nach einer Attacke wiederzuerlangen, ohne dafür Lösegeld bezahlen zu müssen.
- Auch sollen Nutzer über die Funktionsweise von Ransomware und mögliche Gegenmaßnahmen aufgeklärt werden.
- Die Initiative gilt als eines der erfolgreichsten Beispiele für ein Public-Private-Partnership im Bereich der Cybersicherheit.

Gründungspartner der Coalition Against Stalkerware

- Vor dem Hintergrund der wachsenden Bedrohung durch Stalkerware wurde die Coalition Against Stalkerware im November 2019 gegründet.
- Hilfsorganisationen für Opfer häuslicher Gewalt sowie die IT-Sicherheitsgemeinschaft bündeln ihre Erfahrungen sowie ihr Praxis- und Fachwissen aus den Bereichen der Technologie, der Opferarbeit und der Cyber-Rechtsprechung zur Bekämpfung des kriminellen Missbrauchs von Stalkerware.
- Auch soll die Öffentlichkeit für das Thema digitales Stalking und Belästigung sensibilisiert werden.

Coalition Against Stalkerware

Internationale Zusammenarbeit: Europäische Union

- Cyber Resilience Act (CRA):
  - Einreichung zur öffentlichen Konsultation der EU-Kommission
  - Teilnahme und Beitrag zu zwei öffentlichen Anhörungen im EU-Parlament
- ENISA und Cybersecurity-Zertifizierungssysteme:
  - Kaspersky hat an der Konsultation mitgewirkt und einen Blogpost zu diesem Thema veröffentlicht
  - Kaspersky hat zum Europäischen Zertifizierungssystem für Cybersicherheit (EUCC) beigetragen, das auf Comon Criteria (CC) basiert
- EU Cybersecurity Skills Academy:
  - Kaspersky hat eine umfassende Verpflichtungserklärung vorgelegt (Pledge), die verschiedene Schulungs- und Sensibilisierungsmaßnahmen für EU-Bürger, Studierende und Fachleute im Bereich der Cybersicherheit vorsieht (wird derzeit von der Europäischen Kommission geprüft).

- September 2023: Vorlage an den Ad-hoc-Ausschuss zur Ausarbeitung eines umfassenden internationalen Übereinkommens zur Bekämpfung des Einsatzes von Informations- und Kommunikationstechnologien zu kriminellen Zwecken
- Juli 2023: Beitrag zum informellen Dialog im Rahmen der offenen Arbeitsgruppe für die Sicherheit von und bei der Nutzung von ITK
- April 2023: Einreichung beim Global Digital Compact
- März 2023: Stellungnahme von Kaspersky beim Virtuellen Informellen Dialog der Offenen Arbeitsgruppe der Vereinten Nationen (OEWG) 2021-2025 über Entwicklungen im Bereich der Information und Telekommunikation (ITK) im Kontext der internationalen Sicherheit und des Friedens

- IGF 2023:
  - Kaspersky organisierte den Workshop "Ethical principles for the use of AI in Cybersecurity" (Ethische Grundsätze für den Einsatz von KI in der Cybersicherheit); die Kernaussagen des Workshops wurden in die Kyoto IGF Messages (S. 7) aufgenommen
  - Kaspersky nahm an einer Podiumsdiskussion im Rahmen des IGF-Parliamentary Tracks teil
  - Kaspersky präsentierte Multistakeholder-Initiativen auf dem IGF Village
- Kaspersky engagiert sich IGF Policy Network on Artificial Intelligence (PNAI) und hat am Bericht "Strengthening multi-stakeholder approach to global AI governance“ mitgewirkt.
- IGF Afrika/September 2023: Kaspersky trägt zum Programm für Parlamentarier bei

Transparenz

Grundprinzipien von Kaspersky

1. Kaspersky verfolgt das Ziel, jede Malware zu erkennen und abzuwehren, unabhängig von Herkunft, Zweck oder “Sprache”.
2. Für die Zusammenarbeit mit Strafverfolgungsbehörden hat Kaspersky strenge, standardisierte Richtlinien entwickelt und veröffentlich freiwillig halbjährliche Transparenzberichte.
3. Kaspersky setzt auf internationale Zusammenarbeit und engagiert sich in wichtigen Organisationen weltweit, um die Cybersicherheit zu stärken.

Kaspersky Global Transparency Initiative

Cyberthreat-related user data storage and processing

Malicious and suspicious files received from users of Kaspersky products in Europe, North and Latin America, the Middle East, and also countries in Asia-Pacific region are processed and stored in Switzerland.

Transparency Centers

A facility for customers, partners and government stakeholders to review the company's code, software updates and threat detection rules, along with other activities.

Independent reviews

Regular third-party assessment of internal processes to confirm the security of Kaspersky's processes and systems, including:

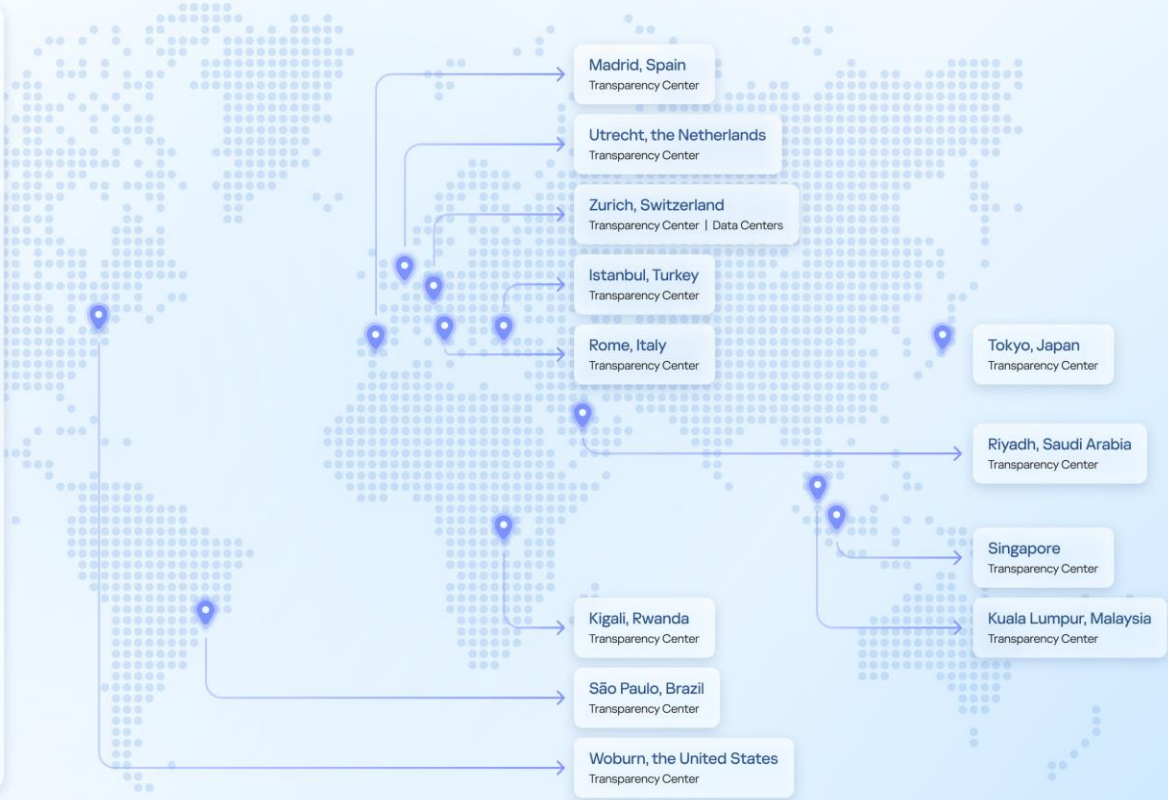
- Regular SOC 2 audits
- ISO 27001 certifications for the company's data systems

Bug bounty program

Increased bug bounties up to $100k for the most critical vulnerabilities aim to engage security researchers to supplement the company's own work in ensuring the security of its solutions.

Transparency reports

Regular updates on how Kaspersky responds to requests from government and law enforcement agencies as well as to personal data-related requests from its own users.



kaspersky bring on the future

Proven. Transparent. Independent.

Neueste Ergebnisse mit Blick auf Vertrauen und Transparenz

1. Erfolgreiches SOC-2 Typ II Audit für den Zeitraum von 6 Monaten (12/2022-5/2023). Ergebnis: Die Prozesse sind vor unberechtigten Änderungen an den Antiviren-Datenbanken geschützt.

2. Re-Zertifizierung der Infrastruktur für die Verarbeitung von Kundendaten nach ISO 27001 zur Bestätigung des Risikomanagementprozesses zum Schutz der Kundendaten.

3. **Die Produkte von Kaspersky wurden in den Katalog der IKT-Sicherheitsprodukte (CPSTIC) aufgenommen, der vom Nationalen Kryptologiezentrum Spaniens (CCN) empfohlen wird.**

4. AV-Comparatives zeichnet Kaspersky Standard als „Produkt des Jahres“ aus. Sowohl die Consumer- als auch die Business-Lösungen werden 2023 vielfach ausgezeichnet.

5. Der Source Code aller On-Premise Produkte kann in den Kaspersky Transparency Centern oder remote überprüft werden.

KES: Qualifiziertes Produkt in der Kategorie „Hoch“ in Spanien

- Kaspersky Endpoint Security (KES) wurde in die Liste der vom *Centro Criptológico Nacional* (Nationales Kryptographie Zentrum - CCN) in Spanien zugelassenen Produkte (CPSTIC) aufgenommen.
- Der Katalog der Sicherheitsprodukte für Informations- und Kommunikationstechnologien (STIC) enthält u. a. eine Liste der zugelassenen Produkte für den Umgang mit sensiblen Informationen und dient als Referenz für die öffentliche Verwaltung in Spanien.
- Zweck dieses Katalogs ist es, den Behörden eine Liste von STIC-Referenzprodukten oder -diensten zur Verfügung zu stellen, deren Sicherheitsfunktionalitäten in Bezug auf den Gegenstand ihrer Anschaffung zertifiziert wurden.
- KES wurde als qualifiziertes Produkt in der Kategorie "Hoch" aufgenommen. Der Abschnitt "Qualifizierte Produkte" umfasst Produkte, die die Sicherheitsanforderungen für den Umgang mit sensiblen Informationen des Nationalen Sicherheitssystems Spaniens (ENS) in einer seiner Kategorien (HOCH, MITTEL und BASIS) erfüllen.

Vielen Dank!

Informationsaustausch, internationale Zusammenarbeit und Transparenz für mehr Cybersicherheit und Resilienz

Jochen Michels Director, Public Affairs, Europe

kaspersky