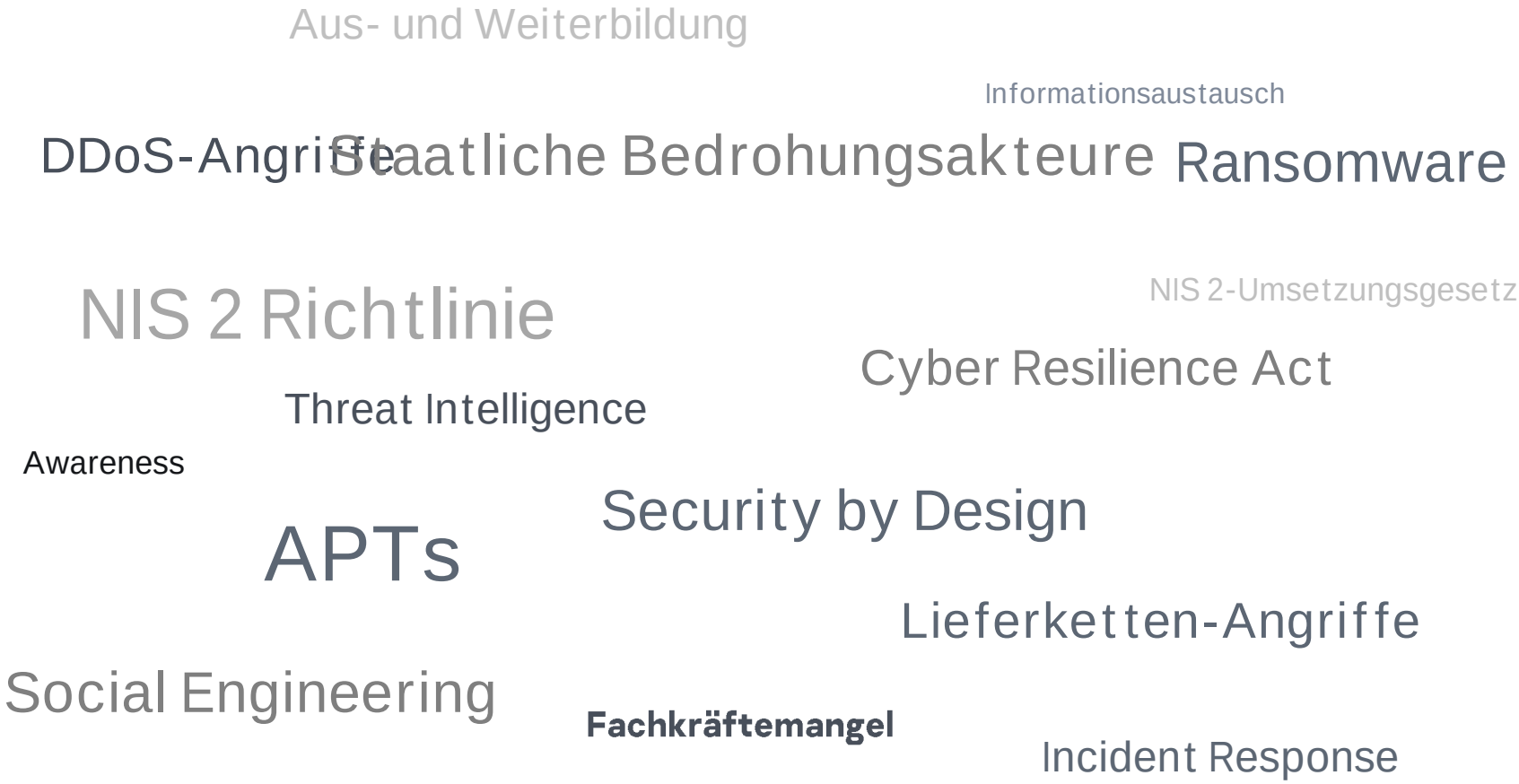
Cyber Immunity – durch Security by Design und Transparenz

KasperskyOS


Aus- und Weiterbildung
Informationsaustausch
DDoS-Angriffe
Staatliche Bedrohungsakteure
Ransomware
NIS 2 Richtlinie
NIS 2-Umsetzungsgesetz
Cyber Resilience Act
Threat Intelligence
Awareness
Security by Design
APTs
Lieferketten-Angriffe
Social Engineering
Fachkräftemangel
Incident Response

Zuwachs an neu entdeckter Schadsoftware

1 Neue Malware pro Tag

1997

1 Neue Malware pro Minute

2006

1 Neue Malware pro Sekunde

2014

411 000 Neue Malware pro Tag

2023

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 schädliche Objekte** auf 18,3 Prozent der industriellen Computer in Deutschland; 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)

Heute: Cybersicherheit

Morgen: Cyber-Immunity

Wir brauchen …

einen Paradigmen-wechsel!

Immanenter Schutz

Security by Design

Reaktiver Schutz

Globale Transparenzinitiative

2 weitere Orte zur Datenverarbeitung

in der Schweiz – weltweit als neutrales Land mit strengen Datenschutzbestimmungen bekannt.

Hier verarbeiten und speichern wir bedrohungsbezogene Nutzerdaten aus Europa, Nord- und Lateinamerika, dem Nahen Osten und mehreren Ländern im asiatisch-pazifischen Raum.

11 Transparenz-zentren

in Brasilien, Italien, Japan, Malaysia, den Niederlanden, Singapur, Ruanda, Spanien der Schweiz, Saudi-Arabien, der Türkei.

2 regelmäßige, unabhängige Überprüfungen durch Dritte

die die Vertrauenswürdigkeit der technischen Praktiken von Kaspersky bestätigen:

- SOC 2 Audit
- ISO 27001 Zertifizierung

8.4$ Millionen Investment

Seit dem Jahr 2018 hat Kaspersky über 8,4 Millionen US-Dollar in das Programm investiert, darunter 5,6 Millionen US-Dollar für die Ausrüstung der Rechenzentren in Zürich.

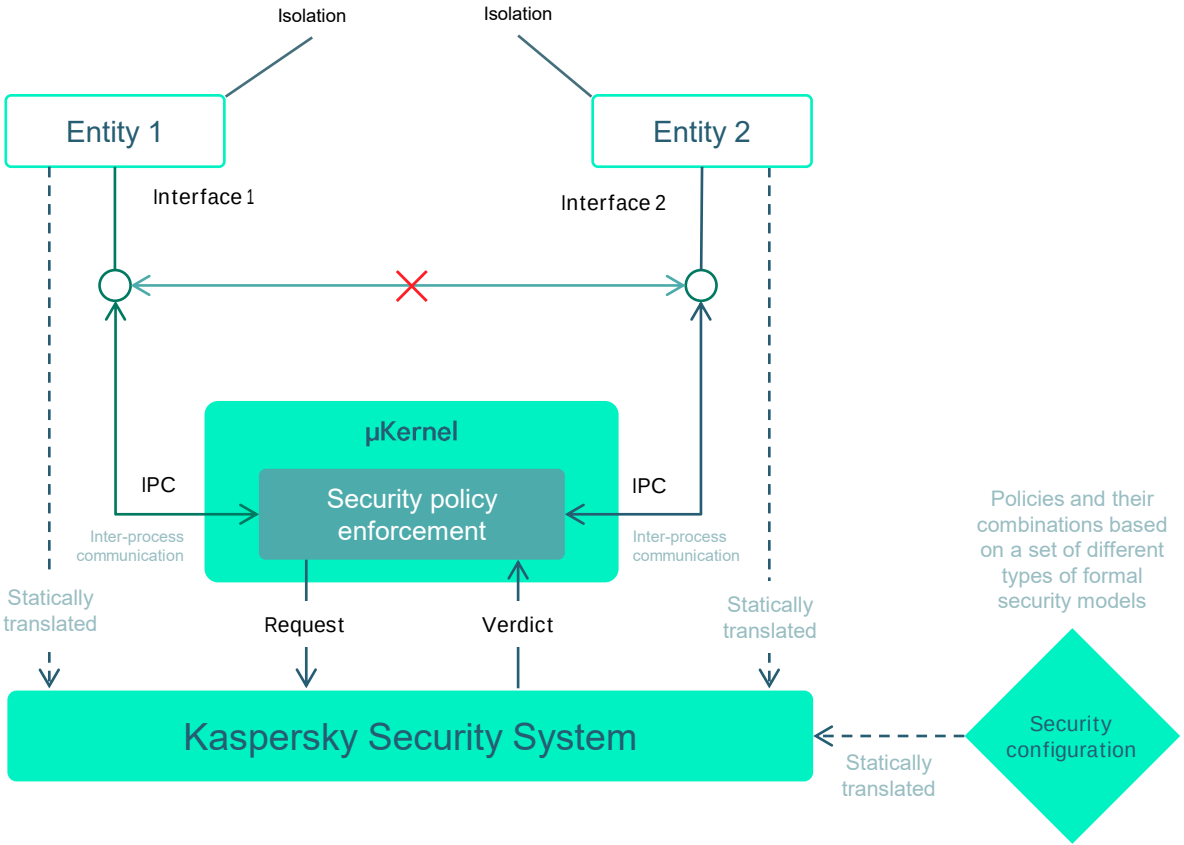
61 Besuche in den Transparenz-zentren

von privaten und öffentlichen Einrichtungen bisher.

59 Bug-Bounty-Auszahlungen

mit einem Gesamtwert in Höhe von 81.750 US-Dollar.

Die wichtigsten Sicherheitskonzepte von KasperskyOS



Besteht aus dem kompakten **µKernel und dem Kaspersky** Security System

Im Inneren ist das Betriebssystem in isolierte und gut kontrollierte **Sicherheitsdomänen unterteilt**

Alle Interaktionen zwischen den Prozessen werden kontrolliert

Alle Aktionen, die nicht durch die vordefinierten Sicherheitsrichtlinien erlaubt sind, werden unterbunden

Unterstützung eines Großteils der allgemein anerkannten Standards **für das Schreiben von** Anwendungen

Warum ein Mikrokernel?

96%

der kritischen Linux-Exploits **würden in einem Mikrokernel**-basierten System keinen kritischen Schweregrad erreichen

57%

der Linux-Exploits **würden auf** einen geringen Schweregrad reduziert, und die meisten von **ihnen würden ganz** verschwinden, wenn das System **auf einem geprüften** Mikrokernel **basieren würde**

29%

von Linux-**Exploits würde allein** durch ein Mikrokernel-basiertes Design verhindert

Source:
Simon Biggs, Damon Lee, Gernot Heiser. 2018. The Jury Is In: Monolithic OS Design Is Flawed: Microkernel-based Designs Improve Security

Die wichtigsten Vorteile

Minimierung von Cyber-Risiken
Die spezifische Architektur der Cyber-**immunen Produkte ermöglicht es, die Risiken** ganzer Klassen von Cyber-Angriffen zu eliminieren.

Reduzierung von IT-Kosten
Cyber-immune Produkte erfordern keine **zusätzlichen Sicherheitsfunktionen bzw.** Tools.

Transparenz and **Flexibilität**
Bietet vollständige Transparenz, flexible Konfiguration von Sicherheitsrichtlinien und **Kontrolle über Interaktionen im gesamten** System.

Anwendungsbereiche

IoT & Industrial IoT

Transportation

Industrial Automation

Virtual Desktop Infrastructure

Corporate Mobile Devices

Vielen Dank - Mehr Infos am Stand 7-310!

KasperskyOS