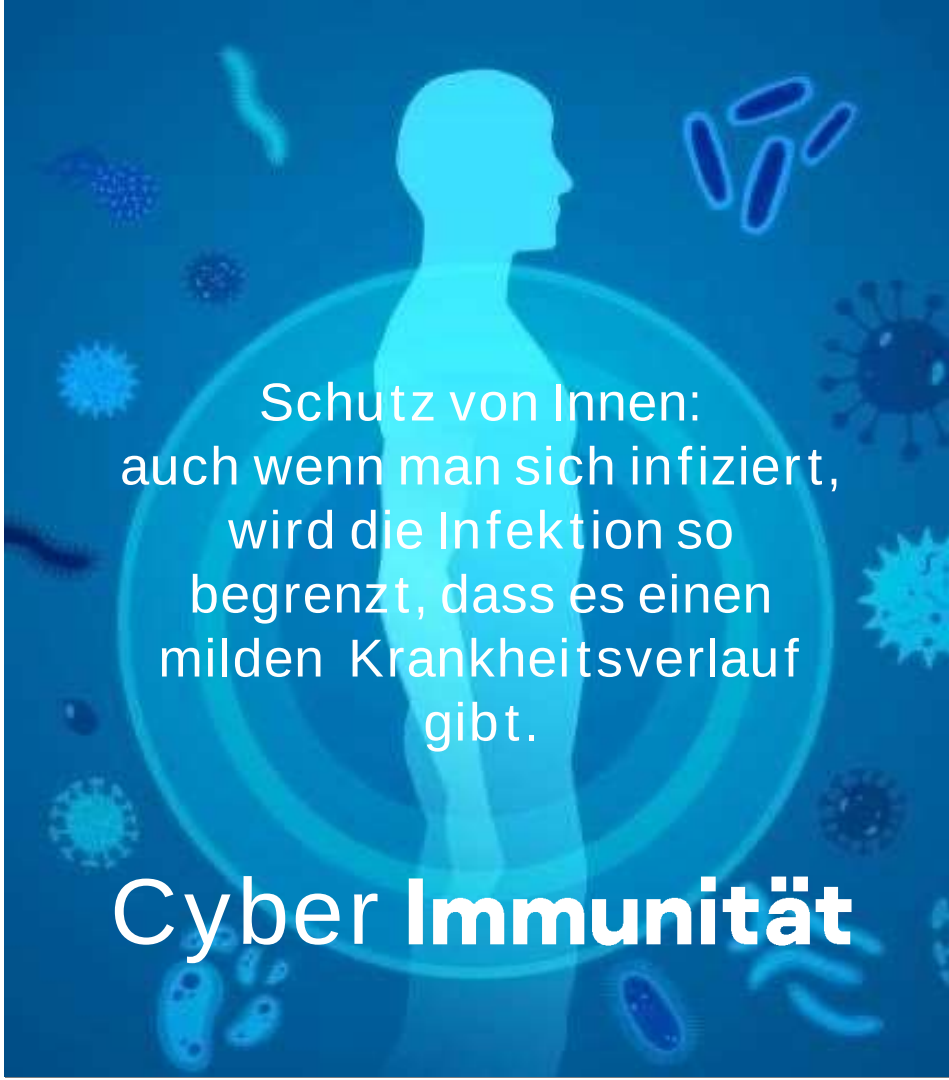
# IT-SECURITY RELOADED – BEGINN DER **ÄRA** DER **CYBERIMMUNITÄT**

itsa 2022

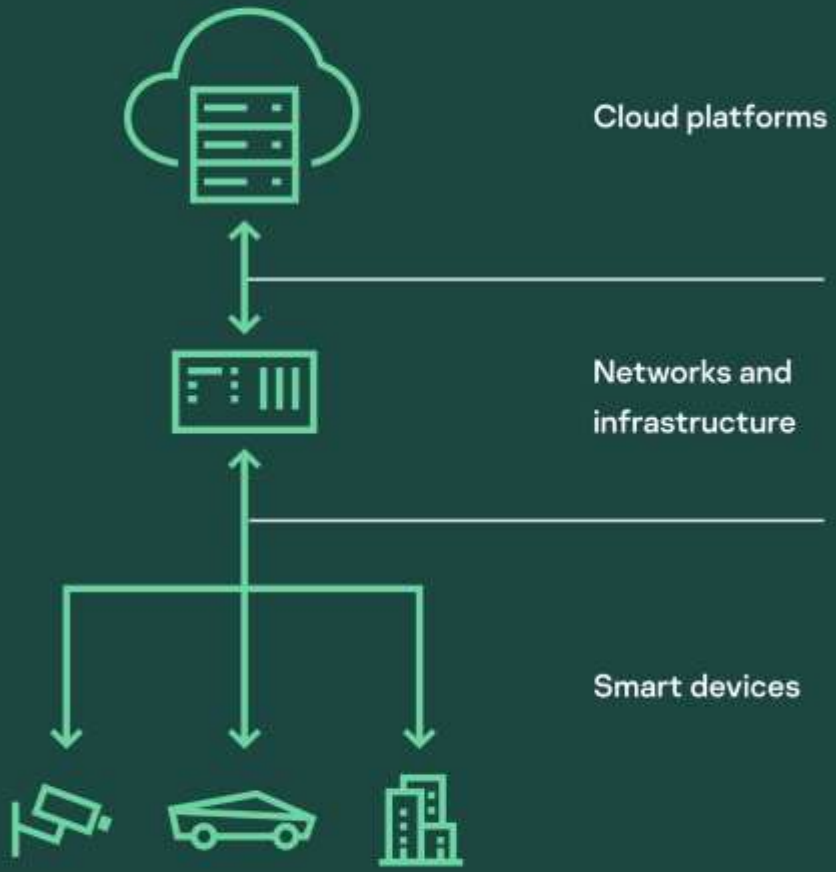
Jochen Michels, Head of Public Affairs Europe, Kaspersky

KasperskyOS

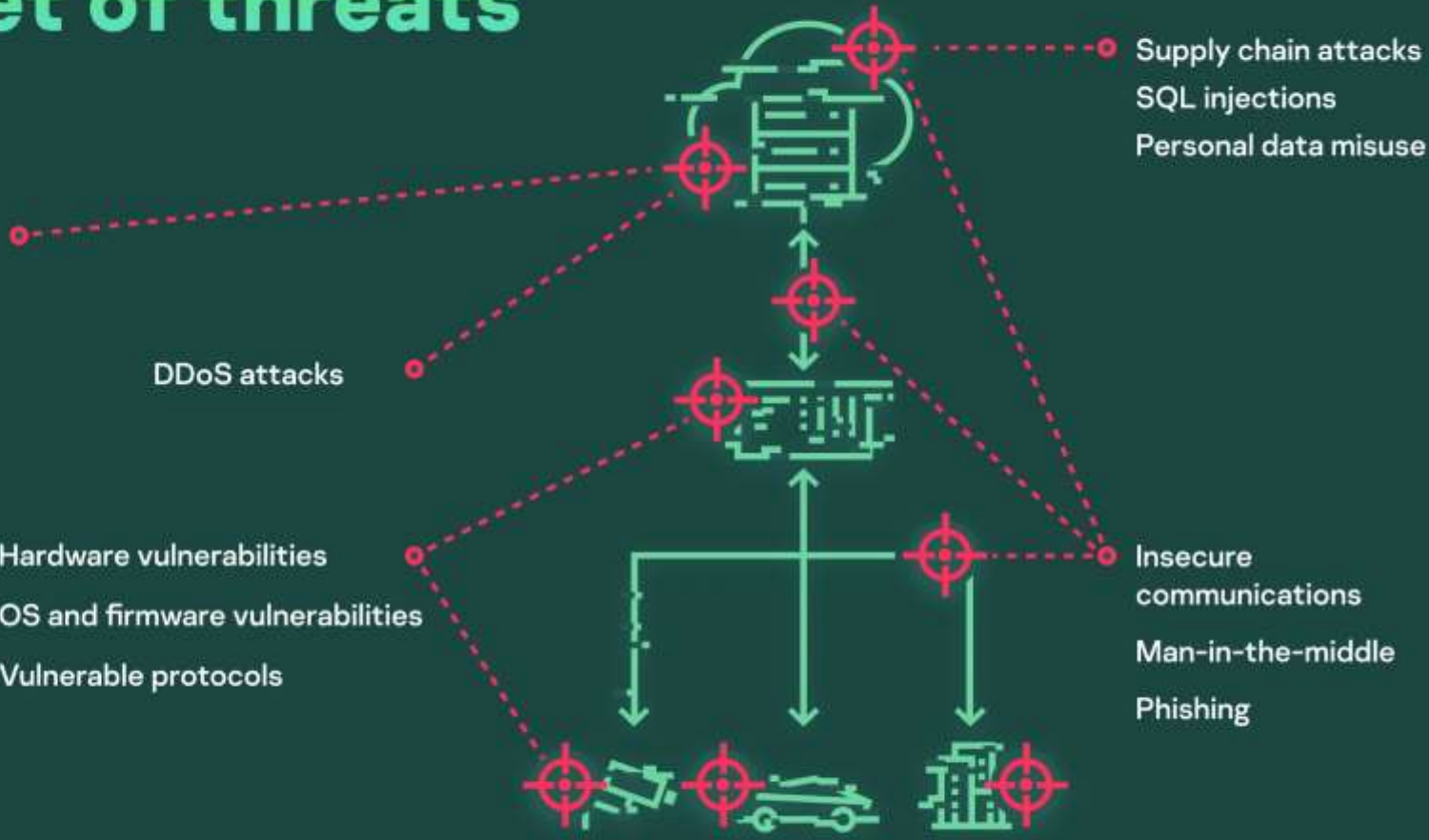
# Cybersicherheit

# Internet of things



# Internet of threats



## Security by Design

Klare Definition der Sicherheitsziele (z. B. Vertraulichkeit der Daten) sowie der Umgebung, in der das System betrieben werden soll

## Isolierung

**Separation der Lösungen** in isolierte Sicherheits-bereiche unter **Berück-**sichtigung der Funktiona-**lität** und des Grades des Vertrauens in jeden dieser Bereiche

## Kontrolle

Strikte Kontrolle des Informationsflusses zwischen Sicherheits-**domänen**, die nur bestimmte Arten von **Interaktionen zulässt**

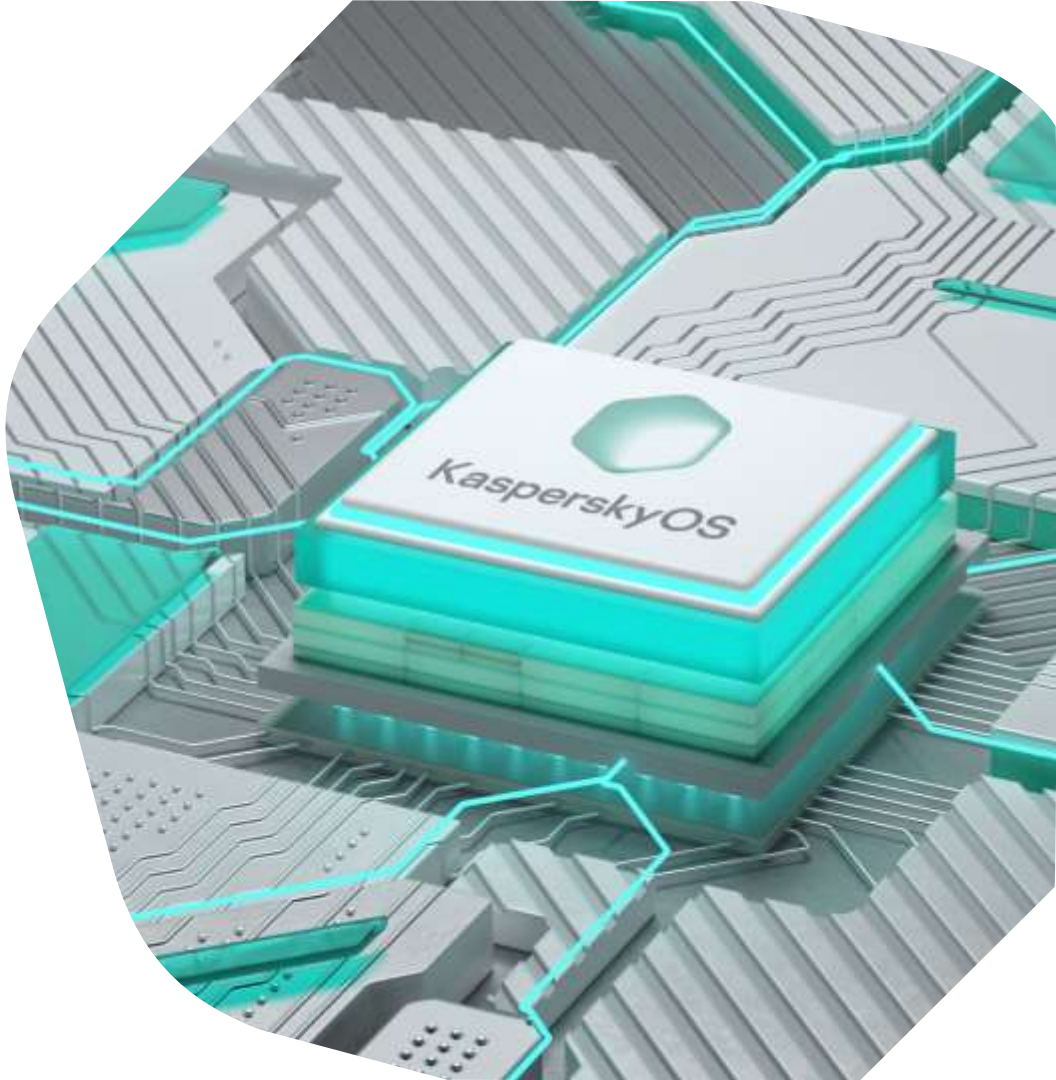
Wie Kasperskys Cyber Immunität umsetzt

# Ein Mikrokernel-Betriebssystem für IT-Systeme mit hohen Anforderungen an die Cybersicherheit

Bietet eine Plattform für die Entwicklung von "Secure by Design"-Lösungen

Schafft eine Umgebung, die es Anwendungen nicht erlaubt, nicht deklarierte Funktionen auszuführen, und verhindert die Ausnutzung von Schwachstellen

Bietet hohe Transparenz, flexible Konfiguration von Sicherheitsrichtlinien und Kontrolle über Interaktionen im gesamten System



# Warum ein Microkernel?



**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%**

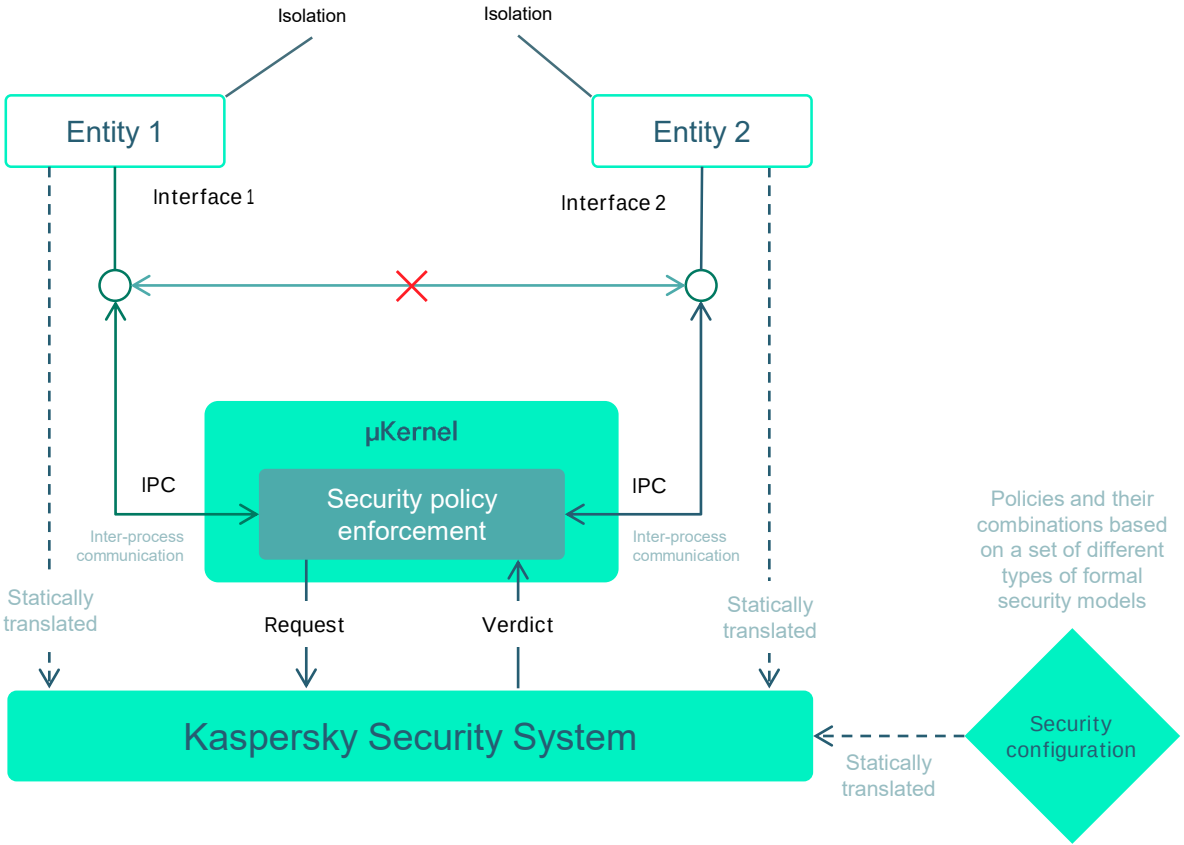
von Linux-Exploits würde allein durch ein Mikrokernel-basiertes Design verhindert, auch ohne Verifizierung

Aus der Sicht der Cybersicherheit ist das monolithische Betriebssystemdesign fehleranfällig und die Hauptursache für die meisten Sicherheitslücken. Es ist an der Zeit, dass die Welt zu einer Betriebssystemstruktur übergeht, die den Sicherheitsanforderungen des 21. Jahrhunderts regrecht wird.

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

# 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, sind verboten

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

# Einsatzgebiete

IoT & Industrial IoT

Transportation

Industrial automation

Virtual desktop infrastructure

Corporate mobile devices

E-Governemnet / Smart City / Smart State

## "Interner" Schutz vor Cyberangriffen

## Ohne zusätzliche (aufgesetzte) Sicherheitstools

# IT-SECURITY RELOADED – BEGINN DER **ÄRA** DER **CYBERIMMUNITÄT**

itsa 2022

Jochen Michels, Head of Public Affairs Europe, Kaspersky

KasperskyOS