Cyber-Immunität schützt vor allen Bedrohungen

Der Kaspersky Thin Client 2.0 basiert auf einem sicheren Betriebssystem nach dem Prinzip «Secure by Design» und ist dadurch immun gegen Cyberbedrohungen aller Art. Er eignet sich für sämtliche Einsatzszenarien, die eine starke Cyber-Resilienz erfordern.

Ob Finanz-, Bildungs- oder Gesundheitswesen, Energieversorgung, Lagerlogistik, Produktion, Behörden oder Detailhandel – Thin Clients sind in den verschiedensten Branchen auf dem Vormarsch. Laut einer Studie von Verified Market Research wird der weltweite Umsatz mit Thin Clients zwischen 2024 und 2031 von 1,14 Milliarden auf 1,31 Milliarden US-Dollar wachsen.

Thin-Client-Umgebungen stehen für kostengünstige Arbeitsplätze und ein gewisses Mass an inhärenter Sicherheit. Aber die gängigen Thin-Client-Infrastrukturen basieren auf Betriebssystemen, die nicht von Anfang an auf Sicherheit getrimmt und somit angreifbar sind. Gleichzeitig arbeiten Cybersecurity-Lösungen traditionell reaktiv: Bei bisher unbekannten Bedrohungen ergibt sich eine Verzögerung zwischen einem Angriff und der angemessenen Abwehrreaktion.

Infrastruktur mit Cyber-Immunität

Der Cybersecurity-Spezialist Kaspersky hat bereits 2012 mit der Entwicklung eines Betriebssystems begonnen, das nach dem Prinzip «Secure by Design» und den Konzepten MILS (Multiple Independent Levels of Security) und FLASK (Flux Advanced Security Kernel) Immunität gegenüber Cyberangriffen auf Betriebssystemebene gewährleistet. Bei der Entwicklung von KasperskyOS wurde bewusst nicht auf bestehende Projekte wie Linux zurückgegriffen. Stattdessen hat Kaspersky das Betriebssystem «from scratch» neu gebaut. Das Resultat ist ein schlankes Mikrokernel-Betriebssystem, das mit rund 100 000 Codezeilen auskommt (zum Vergleich: Der Linux-Kernel besteht aus rund 35 Millionen Zeilen) und über 90 internationale Patente vereint.

Neben dem Secure-by-Design-Ansatz ist die Isolation von Security-Domains ein Kernelement von KasperskyOS: Das Kaspersky Security Module (KSM) als Teil von KasperskyOS berechnet Sicherheitsentscheidungen für jede Interaktion zwischen Systemkomponenten, während der Kernel sie anwendet. Darüber hinaus wird nur ein Teil des angewendeten Codes als vertrauenswürdig angesehen, sodass sich die potenzielle Angriffsfläche auf ein absolutes Minimum reduziert. KasperskyOS kann so auch unbekannte Bedrohungen ausschalten, und dies ganz ohne Beizug separater Cybersecurity-Tools, was die Gesamtkosten (TCO) reduziert. Kurz: KasperskyOS ermöglicht eine cyberimmune Infrastruktur, die mit Regelungen wie Common Criteria, ASPICE oder ISO 26262 konform geht, die Security- und Businesslogik sauber trennt und sich unter anderem für Thin Clients, aber auch für den Einsatz in IoT- und OT-Anwendungen eignet.

Der cyberimmune Kaspersky Thin Client

In Zusammenarbeit mit Centerm, einem weltweit führenden Hersteller von Thin Clients als OEM, hat Kaspersky seine cyberimmune Infrastruktur in Hardware gegossen und auf den Markt gebracht. Der Kaspersky Thin Client, heute bereits in der stark verbesserten Version 2.0 erhältlich, basiert auf KasperskyOS, bietet Anwendern Zugang zu einem hochsicheren Remote-Desktop und ersetzt einen lokalen Arbeitsplatz mit herkömmlichen PCs. Ganz besonders eignet er sich für Branchen, die eine starke Cyber-Resilienz benötigen: Selbst in einer schädlichen Umgebung kann der Client seine Funktionen voll und vertrauenswürdig erfüllen, da KasperskyOS Gerätekompromittierungen ausschliesst. Als kompaktes Gerät spart der Kaspersky Thin Client 2.0 zudem Platz, und die gesamte Thin-Client-Infrastruktur ist einfach zu verwalten und in Anschaffung und Betrieb erschwinglich.

Im deutschsprachigen Raum können Reseller den Kaspersky Thin Client exklusiv bei BOLL Engineering respektive BOLL Europe beziehen. BOLL war schon im Vorfeld der Markteinführung an der Evaluierung des Produkts und der Ausgestaltung der Go-to-Market-Strategie beteiligt und arbeitet eng mit Kaspersky zusammen.

KASPERSKY THIN CLIENT: DIE VORTEILE

- Sicheres Betriebssystem nach dem Prinzip «Secure by Design»
- Immun gegen Cyberbedrohungen
- Gewährleistet höchstmögliche Cyber-Resilienz
- Ermöglicht sicheren Zugang zu Remotedesktop
- Kommt ohne zusätzliche Security-Tools aus
- Erschwingliche, einfach zu verwaltende Infrastruktur

BOLL
IT Security Distribution

BOLL Engineering AG

Jurastrasse 58 I 5430 Wettingen
Tel. 056 437 60 60 I info@boll.ch
www.boll.ch