kaspersky

Unternehmensprofil: unsere Werte, unser Geschäft, unsere Lösungen und Services

August 2024

kaspersky

“Unsere Mission ist einfach – der Aufbau einer sichereren Welt. Wir tun dies, indem wir weltweit führend im Bereich der Cybersicherheit werden. Indem wir Technologie schützen, stellen wir sicher, dass diese frei von Cyberbedrohungen bleibt – und so jedem Menschen nur positive Möglichkeiten bietet.“

„Unendliche Möglichkeiten – für ein sichereres Morgen.“

Eugene Kaspersky, CEO von Kaspersky

Über 25 Jahre Einsatz für eine sicherere Welt

Kaspersky ist ein internationales Unternehmen für Cybersicherheit und digitale Privatsphäre, das seit über 25 Jahren eine sicherere digitale Welt aufbaut. In diesem Zeitraum haben wir unser Portfolio von reiner Endpunktsicherheit hin zu einem umfassenden Schutz von Unternehmen und Verbrauchern entwickelt. Mit einem Team von mehr als 5.000 Fachleuten bauen wir unser Cybersicherheits-Ökosystem weiter aus, mit dem Ziel, alle Sicherheitsanforderungen von Unternehmen und Verbrauchern zu erfüllen, um eine cyberimmune Zukunft zu gewährleisten.

Innovation in der IT-Branche: Das Konzept der Cyber-Immunität

Technologische Meilensteile basierten schon immer auf dem Wunsch nach Innovation. Mit Innovationen geht jedoch das Risiko einher, dass Technologien über ihren beabsichtigten Zweck hinaus missbraucht werden. Auf der Grundlage unserer langjährigen und erfolgreichen Expertise in der Bekämpfung komplexer Cyberkriminalität haben wir bei Kaspersky mit unserem Konzept der Cyber-Immunität Pionierarbeit im Bereich der Sicherheit für die IT-Branche geleistet. Cyber-Immunität zielt darauf ab, cyber-physische Systeme zu schaffen, die von Natur aus sicher und geschützt sind, ein Konzept, das KasperskyOS zugrunde liegt.

Eine Milliarde Geräte wurden bis heute[1] durch Kaspersky geschützt

Die Lösungen von Kaspersky schützen Unternehmen, kritische Infrastrukturen, Regierungen und Verbraucher weltweit vor komplexen Bedrohungen. Dazu gehört der Schutz vor den berüchtigtsten und gefährlichsten Advanced-Persistent-Threat (APT)-Gruppen und Ransomware. Das einzigartige Produktportfolio des Unternehmens umfasst innovative Sicherheitslösungen, die von führendem Endgeräteschutz bis hin zu spezialisierten Sicherheitslösungen und -Services reichen.

Ein umfassendes Ökosystem

Wir verkaufen nicht nur Lösungen – wir bieten ein Ökosystem strategischer Lösungen, die Kunden heute und in Zukunft schützen, während sich ihr Geschäft weiterentwickelt. Wir sind nicht nur ein Anbieter von

[1] Die Zahl basiert auf den Daten des Kaspersky Security Network (KSN) zur automatischen Malware-Analyse und umfasst Datensätze ab 2011, als das System eingeführt wurde.

Services und Produkten – wir sind ein Partner. Wir analysieren die Geschäftsbedarfe eines Unternehmens, brechen die Anforderungen herunter und finden die besten Lösungen für ein stabiles Wachstum und eine stabile Entwicklung, unabhängig von seiner Größe, seinem Bereich und seiner Expertise. Unsere Produkte und Dienstleistungen basieren auf umfassender und kontinuierlicher Bedrohungensforschung und Entwicklungsarbeit; mehr als die Hälfte unserer 5.000 Mitarbeiter sind F&E-Spezialisten. Dass wir der meistgetestete und meistausgezeichnete Anbieter von Cybersicherheitslösungen auf der Welt sind belegt, dass diese einzigartige Zusammensetzung erfolgreich ist.

Unser Portfolio ist darauf ausgerichtet, Unternehmen jeder Größe zu unterstützen, von kleinen lokalen Unternehmen bis hin zu globalen Großkonzernen. Wir wissen, dass sich mit der Veränderung und dem Wachstum von Unternehmen, der Einführung neuer Technologien, der Bewältigung schwerwiegender Sicherheitsherausforderungen und dem Zugang zu mehr Ressourcen auch die Anforderungen an die Cybersicherheit ändern und wachsen sowie zusätzliche Optionen erfordern. Unser stufenweiser Ansatz steht im Einklang mit dieser natürlichen Entwicklung.

Threat Intelligence mit globaler Reichweite

Kaspersky ist in mehr als 200 Ländern und Territorien tätig und verfügt daher über Echtzeitinformationen aus der ganzen Welt, um seine Nutzer vor Bedrohungen zu schützen, die andere Anbieter möglicherweise übersehen. Wir sind daher die Ersten, die von neuen Bedrohungen erfahren. Unsere globale Abdeckung hilft uns, ihre Ausbreitung schnell zu verhindern.

Ein einzigartiges Team von Sicherheitsexperten

Unsere äußerst erfahrenen Expertenteams arbeiten in fünf Kompetenzzentren rund um die Uhr an der Bekämpfung von Massenangriffen, Malware, gezielten und APT-Angriffen sowie branchen- und infrastrukturspezifischen Bedrohungen, um unsere Kunden zu schützen.

- Das **Kaspersky Global Research and Analysis Team (GReAT)** erforscht und entdeckt die raffiniertesten Bedrohungen (von Duqu, Equation oder Carbanak bis hin zur neuesten Bedrohung Operation Triangulation)
- **Kaspersky Threat Research** forscht im Bereich Anti-Malware und Content Filtering, entwickelt Schlüsseltechnologien zur Bedrohungsabwehr und trägt zu unseren einzigartigen SSDLC- und Secure by Design-Methoden bei.
- Das **Kaspersky AI Technology Research Center** befasst sich mit allgemeiner KI-Forschung und KI-gestützter Bedrohungserkennung und Lösungen.
- **Kaspersky Security Services** umfassen MDR, Incident Response, Security Assessments, SOC Consulting und Digital Footprint Intelligence.
- Das **Kaspersky ICS CERT** zeichnet sich im Bereich der industriellen Infrastrukturen aus, führt OT-Bedrohungsanalysen, Schwachstellenforschung und -bewertung durch und arbeitet mit Technologieverbänden und Produktanbietern zusammen, um hohe Sicherheitsstandards für Next-Generation-Technologien zu schaffen.

Die in den Kaspersky Expertise Centern geleistete Arbeit fließt in unsere Lösungen und Services ein, damit unsere Kunden sicher sind und selbst den raffiniertesten Bedrohungen einen Schritt voraus sind.

kaspersky

Kombination von Sicherheitsexpertise mit der Leistungsfähigkeit von Künstlicher Intelligenz

Künstliche Intelligenz (KI) ist auf dem Vormarsch und revolutioniert viele Branchen – von intelligenten Haushaltsgeräten bis hin zu Robotern in der Produktion und im Geschäftsleben. Kaspersky verfügt über umfangreiche Erfahrungen mit KI und setzt sie schon seit fast 20 Jahren zur Lösung spezifischer Probleme ein.

KI-Technologien sind ein integraler Bestandteil unserer Lösungen und Produkte und finden ihren Platz sowohl in Kasperskys eigener Infrastruktur als auch in kundenseitigen Lösungen. Beispielsweise:

- Kaspersky Security Network (KSN) – ein Cloud-Datenverarbeitungszentrum, das globale Bedrohungsdaten sammelt, neue Malware erkennt und dabei hilft, neue Erkennungsmodelle für den späteren Einsatz vor Ort zu erstellen, die in mehrere Kaspersky-Produkte integriert sind.
- Kaspersky Industrial CyberSecurity (KICS) und Machine Learning for Anomaly Detection (MLAD) nutzen KI-Algorithmen, um indirekte Angriffsindikatoren und subtile Aktivitätsanomalien in hochspezifischen industriellen Umgebungen zu erkennen.
- Die Managed Detection and Response (MDR)-Plattform wird durch den KI-basierten Autoanalysten unterstützt, der mit Alarmen des SOC-Teams gespeist wird, um diese später automatisch zu verarbeiten und die SOC-Analysten von einem erheblichen Teil manueller Arbeit zu entlasten.

Wir sind zum derzeitigen Stand der Entwicklung von KI überzeugt davon, dass die effektivsten Lösungen entstehen, wenn Menschen und Maschinen zusammenarbeiten und ihre Stärken gegenseitig maximieren. Unser Team im Kaspersky AI Technology Research Center arbeitet seit fast zwei Jahrzehnten mit KI in der Cybersicherheit und ethischer KI, um ein breites Spektrum an Bedrohungen zu entdecken und zu bekämpfen. Ihre Arbeit ist der Beweis dafür, dass die Verbindung von KI-Fähigkeiten mit menschlichem Fachwissen und umfassenden Bedrohungsdaten aus Big Data die effektivste und zuverlässigste Sicherheit schafft.

Höchste Qualität bestätigt durch zahlreiche Tests und Auszeichnungen

Unsere Produkte werden regelmäßig externen Überprüfungen und Tests unterzogen und erhalten die höchsten Auszeichnungen und Anerkennungen. Mit über 600[2] Branchenauszeichnungen für unsere Sicherheitslösungen ist Kaspersky zudem einer der anerkanntesten Sicherheitsanbieter auf dem Markt. Unsere Technologien und Prozesse werden von einigen der weltweit angesehensten Organisationen umfassend geprüft und zertifiziert, um die beste Sicherheit für unsere Kunden zu gewährleisten.

Weitere Informationen über unabhängige Bewertungen und Zertifizierungen

Kaspersky arbeitet kontinuierlich mit weltweit anerkannten Organisationen zusammen, um seine internen Prozesse unabhängig überprüfen zu lassen, darunter:

- Service Organization Control for Service Organizations (SOC 2) Typ 1, das von einer der vier großen Wirtschaftsprüfungsgesellschaften durchgeführt, wird seit 2019 durchgeführt. Im Jahr 2023 bestand Kaspersky außerdem ein umfassendes SOC-Typ-2-Audit, das die Wirksamkeit der zum Schutz des Prozesses der Entwicklung von Antiviren-Datenbanken implementierten Kontrollen bestätigt.

[2] Die Zahl umfasst unabhängige Testergebnisse von Unternehmens- und Verbraucherprodukten im Zeitraum 2013-2023.

- Die Zertifizierung nach ISO/IEC 27001:2013, dem internationalen Standard, der Best Practices für Informationssicherheits-Managementsysteme festlegt, wurde von Kaspersky im Jahr 2020 erlangt. Eine Re-Zertifizierung fand im Jahr 2022 mit erweitertem Geltungsbereich statt.

Globale Transparenzinitiative: Wir sind transparent in unserer Arbeitsweise und wie wir Verbraucher und Unternehmen schützen

Kaspersky ist das erste Cybersicherheitsunternehmen, das seinen Quellcode öffentlich zur externen Überprüfung bereitstellt und Kunden sowie Partnern seine Software Bill of Materials (SBOM) zur Verfügung stellt. Um das Vertrauen in das hohe Niveau unseres Datenschutzes zu stärken, ermöglicht es unser internationales Netzwerk von Transparenzzentren Interessenvertretern, sich über unsere internen Prozesse und Datenmanagementpraktiken zu informieren.

Weitere Informationen zur Globalen Transparenzinitiative

Kaspersky verpflichtet sich, seine Kunden vor Cyberbedrohungen zu schützen, unabhängig von deren Ursprung oder Zweck. Die Globale Transparenzinitiative (GTI) des Unternehmens hat zum Ziel, die breitere Informationssicherheitsgemeinschaft und andere Interessengruppen in die Validierung und Verifizierung der Vertrauenswürdigkeit seiner Produkte, internen Prozesse und Geschäftsabläufe einzubeziehen. Kaspersky führt zudem zusätzliche Mechanismen der Rechenschaftspflicht ein, über die das Unternehmen weiter nachweist, dass es alle Sicherheitsprobleme umgehend und gründlich angeht. Weitere Informationen zur Geschichte der Globalen Transparenzinitiative und ihrer Expansion weltweit unter https://gti.kaspersky.com/.

Die Globale Transparenzinitiative von Kaspersky umfasst eine Reihe umsetzbarer und konkreter Maßnahmen:

- **Externe Überprüfung** des Quellcodes des Unternehmens, Softwareupdates und Bedrohungserkennungsregeln
- **Unabhängige Überprüfung** der sicheren Entwicklung der Lifecycle-Prozesse sowie der Strategien zur Risikominimierung in der Software-Entwicklungskette
- **Verlagerung der cyberbedrohungsbezogenen Datenspeicherung und -verarbeitung in die Schweiz** für Kunden in Europa, den Nord- und Lateinamerika, dem Mittleren Osten sowie mehreren Ländern im asiatisch-pazifischen Raum.
- **Globale Transparenzzentren weltweit,** um Sicherheitsbedenken gemeinsam mit Kunden, vertrauenswürdigen Partnern und Regierungsvertretern anzugehen. Die elf Kaspersky Transparenzzentren befinden sich in den Regionen META, Asien-Pazifik, Europa und Lateinamerika.
- **Die Prämien für das Bug Bounty Programm** wurden im Rahmen des Vulnerability Disclosure-Programms von Kaspersky auf bis zu 100.000 US-Dollar für schwerwiegende Schwachstellen erhöht. Seit 2022 betreibt Kaspersky sein öffentliches Bug-Bounty-Programm auf der Yogosha-Plattform. Außerdem unterstützen wir das Disclose.io-Framework, das Sicherheitsforschern, die sich über negative rechtliche Folgen ihrer Entdeckungen Sorgen machen, einen Safe Harbor bietet.
- **Transparenz des Unternehmens in seiner verantwortungsvollen Offenlegung von Sicherheitslücken**, indem ethische Grundsätze veröffentlicht wurden.
- **Transparenzberichte**, in denen die Anzahl der Anfragen von Strafverfolgungs- und Regierungsbehörden nach Informationen über Nutzerdaten, Fachwissen und technische Informationen zur Untersuchung von Bedrohungen offengelegt wird.

- **Start des Cyber Capacity Building Programs**, eines speziellen Schulungskurses (auch online verfügbar) zur Bewertung der Produktsicherheit für mehr Sicherheit und Cyber-Resilienz des IKT-Ökosystems.

Bildung und Zusammenarbeit für ein sichereres digitales Zeitalter

Kaspersky arbeitet ständig daran, seine Nutzer über die sich entwickelnde Cyberbedrohungslandschaft aufzuklären, und spricht auf verständliche Weise über komplexe digitale Themen. Das Unternehmen arbeitet daran, die Online-Sicherheit von Kindern zu verbessern, und unterstützt die Entwicklung junger Talente, indem es zur internationalen IT-Community beiträgt. Kaspersky leitet zudem weltweite Verbände und gemeinsame Projekte zum Schutz Bedürftiger.

Weitere Informationen zu unserer Rolle in der weltweiten IT-Sicherheits-Community

Zusammenarbeit ist der effektivste Weg, um eine sicherere Welt aufzubauen und Cyberkriminelle zu bekämpfen. Wir glauben, dass es keine Grenzen für Sicherheit gibt. Daher teilen wir unsere Expertise, unser Wissen und unsere technischen Erkenntnisse mit der weltweiten Sicherheitsgemeinschaft. Unser Unternehmen hat an Untersuchungen mit Adobe, AlienVault Labs, Novetta, CrowdStrike, OpenDNS und weiteren teilgenommen. Darüber hinaus wurde Kaspersky in die Liste der Top Contributors für Sicherheitslücken von Microsoft aufgenommen.

Wir sind stolz darauf, mit globalen IT-Sicherheitsanbietern, internationalen Organisationen und nationalen sowie regionalen Strafverfolgungsbehörden auf der ganzen Welt bei der Bekämpfung der Internetkriminalität zusammenzuarbeiten.

Zusammen mit Strafverfolgungsbehörden und CERTs weltweit, kooperiert Kaspersky mit INTERPOL zur gemeinsamen Bekämpfung von Internetkriminalität. Das Unternehmen bietet der Organisation Personalunterstützung, Schulungen und Bedrohungsdaten in Bezug auf die neuesten Cyberkriminalitätsaktivitäten. Konkret haben Kaspersky-Forscher seit 2019 Schulungen für INTERPOL-Vollzugsbeamte durchgeführt, darunter mehr als 10 Cybersecurity-Schulungen.

Kaspersky ist zudem Mitglied in Initiativen und Organisationen wie Securing Smart Cities, dem Industrial Internet Consortium, AUTOSAR, International Telecommunication Union und International Organization for Standardization. Wir sind Gründungsmitglied der Coalition Against Stalkerware und der NoMoreRansom-Initiative und nehmen als Partner am Genfer Dialog teil – einer Gruppe von Interessenvertretern, die einen internationalen Prozess und Dialog über die Sicherheit digitaler Produkte führt. Wir nehmen an gemeinsamen Untersuchungen von Cyberbedrohungen teil und führen Schulungen für Cybersicherheitsspezialisten und internationale Polizeiorganisationen durch. So hat beispielsweise die Zusammenarbeit zwischen der niederländischen Polizei und Kaspersky zur Verhaftung der hinter den Coinvault-Ransomware-Attacken stehenden Verdächtigen geführt.

Kaspersky beteiligt sich auch proaktiv an UN-Initiativen wie Global Digital Compact, der Open-Ended Working Group on the Security and Use of ICT und dem Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of ICT for Criminal Purposes. Kaspersky nimmt zudem regelmäßig am Internet Governance Forum (IGF) unter der Schirmherrschaft der Vereinten Nationen teil. Auf dem IGF 2023 (Kyoto, Japan) organisierte Kaspersky den Workshop "Ethical principles for the use of AI in Cybersecurity" und nahm am IGF Parliamentary Track teil. Dort schlug das Unternehmen sechs Grundsätze für den ethischen Einsatz von KI in der Cybersicherheitsbranche vor.

kaspersky

Weitere Informationen zu unseren Bildungsinitiativen

Wir sind davon überzeugt, dass die Ermutigung zum Dialog und die Einführung von Bildungsprogrammen essenziell für die internationale Zusammenarbeit im Kampf gegen Cyberkriminalität sind. Daher betreiben wir die Kaspersky Academy: ein internationales Bildungsprojekt, das 2010 ins Leben gerufen wurde. Im Rahmen dieses Programms fördern wir das Wissen über Cybersicherheit weltweit, indem wir junge Talente in der IT fördern und zur Entwicklung erstklassiger Bildungsprogramme für Cybersicherheit beitragen.

Kaspersky veranstaltet zudem den Secur'IT Cup – einen globalen Wettbewerb, an dem Studenten aus aller Welt und aus unterschiedlichen akademischen Bereichen teilnehmen können. Die Teilnehmer haben die Chance, 10.000 US-Dollar zu gewinnen; sie profitieren darüber hinaus vom Wettbewerb mit gleichgesinnten Studenten und erhalten einen Einblick in eine zukunftsträchtige Branche. So haben sie die Möglichkeit, ihre eigenen Projektideen einzubringen, um zur Lösung globaler Cybersicherheitsprobleme beizutragen.

Um jungen Talenten das breite Wissen über berufliche Laufbahnen im Bereich Cybersicherheit zu vermitteln und ihre zukünftige IT-Karriere anschaulicher zu gestalten, hat Kaspersky außerdem das Projekt Tech Valley ins Leben gerufen, das sich auf erfahrene Wissenschaftler und Studenten konzentriert. 2023 hat Kaspersky Academy die Kaspersky Academy Alliance ins Leben gerufen, ein spezielles Programm für Universitäten, das die Cybersecurity-Expertise und die neuesten Kaspersky-Technologien in die Lehre integriert, um die akademischen Leistungen der Studenten zu verbessern.

Im gleichen Jahr kündigte Kaspersky außerdem sein Projekt „Kids‘ Cyber Resilience“ an. Das Ziel dieses Projekts besteht darin, einen kollaborativen und proaktiven Ansatz für Online-Sicherheit zu etablieren und Kindern dabei zu helfen, mit Stress umzugehen und mit Herausforderungen in der digitalen Umgebung umzugehen. 2024 veröffentlichte Kaspersky außerdem das Buch "Cybersecurity Alphabet" für Kinder im Alter von 5-12 Jahren. In diesem Buch lernen diese neue Technologien kennen, erfahren die wichtigsten Regeln der Cyber-Hygiene, finden heraus, wie sie Online-Bedrohungen vermeiden und die Tricks von Betrügern erkennen können.

Neben der Aufklärung der Kinder selbst werden Eltern und Pädagogen Wissen und Tools zur Verfügung gestellt, mit denen sie Probleme wie Stress oder Unbehagen zu erkennen sowie potenzielle Cyber-Risiken zu verringern. Weiterhin bietet das Projekt Unterstützung für diejenigen, die von Cyber-Mobbing und anderen Formen negativer negativen Online-Erfahrungen betroffen sind. Die Kaspersky-Experten tragen auch mit Lernmaterialien für Junior High Schools bei.

Darüber hinaus führt das Unternehmen Kaspersky Expert Trainings durch, die sich an Fachleute richten und ihnen helfen, effektive Strategien zur Erkennung und Abwehr von Bedrohungen zu erlernen, um die sich ständig weiter entwickelnden Gefahren der heutigen Cyber-Realität zu bekämpfen.

Weitere Informationen zu unseren sozialen Projekten

In unserer Bemühung, eine sicherere Zukunft zu schaffen, sorgen wir uns nicht nur digital um das Wohlergehen der Welt. Zu den Kernbereiche der nachhaltigen Entwicklung von Kaspersky gehören die Umweltverträglichkeit unserer Infrastruktur, unserer Geschäftsaktivitäten und Produkte, Mitarbeiterpflege, Inklusion und die Verfügbarkeit von Technologien. Das Unternehmen veröffentlicht seine Nachhaltigkeitsberichte seit 2023 und erstellt sie nach den internationalen GRI- und SASB-Standards. Der neueste Bericht, der die Ergebnisse für das zweite Halbjahr 2022 und 2023 enthält, ist unter https://esg.kaspersky.com/en/ verfügbar.

Kaspersky hat die Online-Community ‚Women in Cybersecurity‘ gegründet, die dazu beiträgt, die Karriere von Frauen, die in die Cybersicherheitsbranche einsteigen, und von Frauen, die bereits in diesem Bereich tätig sind, zu beschleunigen. Darüber hinaus haben wir das digitale Projekt ‚Empower Women‘ initiiert, mit

dem Ziel, durch Wissensaustausch weitere Brücken zwischen Frauen und Männern auf allen Ebenen des Unternehmens zu schlagen. Dies trägt dazu bei, ein Arbeitsumfeld zu schaffen, in dem alle ihr volles Potenzial entfalten können – unabhängig vom Geschlecht.

Kaspersky spielt zudem beim Schutz vor Stalkerware eine Vorreiterrolle. Stalkerware ist eine kommerzielle Spyware, die zwar als legal gilt, aber zur heimlichen Überwachung und Verfolgung der Geräteaktivitäten eines Partners verwendet werden kann und oft zu Missbrauch in Privathaushalten führt. Kaspersky ist das erste Unternehmen in der Branche, das diesbezüglich sein Produkt aktualisiert hat. Das Verbraucherportfolio von Kaspersky hat einen Privacy Alert inkludiert, der Nutzer warnt, wenn ihre privaten Daten von Dritten überwacht werden.

Im Jahr 2019 haben Kaspersky und neun weitere Organisationen, die in der IT-Sicherheitsbranche oder mit Betroffenen und Tätern im Bereich Stalkerware arbeiten, die Koalition gegen Stalkerware ins Leben gerufen, eine globale Initiative zum Schutz vor Stalking und häuslicher Gewalt. Bis heute vereint die Koalition mehr als 40 Geschäftspartner und wird von INTERPOL unterstützt. Darüber hinaus unterstützt Kaspersky Non-Profit Organisationen, die mit Betroffenen häuslichen Missbrauchs arbeiten.

Kaspersky war Partner des EU-weiten Projekts „DeStalk“ mit einer Laufzeit von 2021-2023, das die Europäische Kommission mit ihrem Programm „Rechte, Gleichstellung und Unionsbürgerschaft“ unterstützt. DeStalk befasst sich mit den Themen Cybergewalt und Stalkerware, die neue, weit verbreitete und versteckte Formen geschlechtsspezifischer Online-Gewalt darstellen.