Wie Sie der Komplexität die Stirn bieten

Umgang mit komplexen Cybervorfällen, die von modernen hochentwickelten Bedrohungen ausgehen

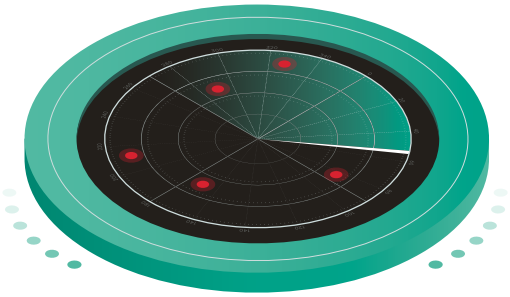
kaspersky BRING ON THE FUTURE

Auch wenn es nicht immer möglich ist, eine Bedrohung zu stoppen, bevor sie in Ihren Perimeter eindringt, sind wir in der Lage, eine weitere Ausbreitung des Angriffs zu verhindern und potentielle Schäden abzuwenden oder zumindest zu begrenzen. Aber gerade bei komplexen oder gezielten Angriffen kommt es entscheidend auf eine schnelle Reaktion an.

Komplexe Vorfälle sind sehr spezifische Bedrohungen, weil sie in der Regel viele Aspekte der Infrastruktur innerhalb der angegriffenen Organisation betreffen. Genau das ist das Dilemma: Wo soll man anfangen, wenn alles gleichermaßen wichtig erscheint?

In diesem Whitepaper möchten wir die fünf größten Hindernisse für die erfolgreiche Bewältigung eines komplexen Vorfalls erörtern. Zunächst soll es aber um das Konzept der Komplexität gehen, und was sie für Cybersicherheitsexperten bedeutet.

Was versteht man eigentlich unter einem komplexen Vorfall?



Im Gegensatz zu einem einfachen lässt sich ein komplexer Vorfall klarer definieren. Die globale Covid-19-Pandemie ist ein anschauliches Beispiel für einen komplexen Vorfall, denn sie betrifft gleich mehrere Systeme: Länder, Organisationen (Behörden und Unternehmen), Kommunen, Schulen, Branchen, Familien und Einzelpersonen. Ganz zu schweigen davon, dass das Virus komplexe Vorgänge im Körper der erkrankten Menschen auslöst; seine Nebenwirkungen reichen von einer Beeinträchtigung des Atmungssystem bis zum kardiovaskulären, renalen, dermatologischen, neurologischen, immunologischen und sogar psychiatrischen System.

Komplexer Cyberspace, komplexe Bedrohungslage, komplexe Cybervorfälle – eine unausweichliche Verkettung?

Man kann sagen, dass die zunehmende Komplexität der Cybervorfälle in direktem Zusammenhang mit der wachsenden Komplexität der IT-Systeme in Unternehmen und tatsächlich auch des Cyberspace selbst steht. Laut einem Bericht der ENISA (der Agentur der Europäischen Union für Cybersicherheit) mit dem Titel *Emerging Trends January 2019 to April 2020 Threat Landscape Report* „ermöglicht die Vernetzung verschiedener Systeme und Netzwerke, dass sich Cybervorfälle schnell und weit ausbreiten, was die Einschätzung und Eindämmung von Cyberrisiken zunehmend erschwert". Mit anderen Worten: Je komplexer die IT-Infrastruktur eines Unternehmens, desto größer das Risiko eines komplexen Cyberangriffs. Und damit verschärft sich die Situation gerade für Großunternehmen, die ihrem Wesen nach immer auch komplex sind.

Doch der offensichtlich erscheinende Zusammenhang zwischen komplexen Umgebungen und komplexen Vorfällen geht über das komplexe IT-System von Großunternehmen hinaus. Laut ISO/IEC 27032:2012 ist der Cyberspace selbst eine „komplexe Umgebung, die sich aus der Interaktion von Menschen, Software und Services im Internet mithilfe von damit verbundenen technischen Geräten und Netzwerken ergibt und die in keiner physischen Form existiert". Anders ausgedrückt, sind wir mit drei Ebenen von Komplexität konfrontiert: dem Cyberspace, der IT-Umgebung des

Unternehmens und den Cybervorfällen. Erschwerend kommt hinzu, dass diese drei Ebenen miteinander verbunden und voneinander abhängig sind und jede von ihnen die eigenen Ziele durch wiederum mehr Komplexität zu erreichen sucht.

Cyberspace: Zunehmende Abhängigkeit von vernetzten Geräten, Systemen und Prozessen im Beruflichen wie im Privaten und die daraus resultierende wachsende Komplexität der Umgebungen

IT-Umgebungen in Unternehmen: Größere Angriffsfläche als Folge der steigenden Zahl von vernetzten Geräten, Systemen und Prozessen (einschließlich der Lieferkette). Gleichzeitig werden Cybervorfälle und auch die Abwehrmaßnahmen immer komplexer.

Die Bedrohungslage und deren Akteure: Reagieren einerseits auf die zunehmende Komplexität sowohl im Cyberspace als auch in Unternehmensumgebungen und nutzen andererseits diese Komplexität gezielt aus, um sehr ausgeklügelte, hochentwickelte Angriffe zu lancieren (mit einer horizontalen Infiltrierung in einem Ausmaß, das zu Zeiten einfach gestalteter Zielsysteme gar nicht denkbar gewesen wäre).

Tatsache ist aber auch, dass von diesen dreien die Bedrohungsakteure als Erste Wege gefunden haben, um die Barrieren der Komplexität zu überwinden – unter anderem durch den Einsatz von Malware-as-a-Service:

„Die Einstiegshürden werden von den Neueinsteigern unter den Cyberkriminellen schnell überwunden, weil die Angreifer über eine ganze Reihe von (technischen) Fähigkeiten und erheblichen Ressourcen verfügen, seit Malware und Malware-as-a-Service über die unterschiedlichsten Quellen (wie Darknet und Deep Web) immer einfacher und günstiger zu haben sind. So steht eine Vielzahl an modernen Techniken und Tools zur Verfügung (z. B. Social-Engineering-Techniken und Zero-Day-Exploit-Programme), die Cyberkriminelle nutzen können, um hochentwickelte gezielte Angriffe zu starten."

Papastergiou, S., Mouratidis, H. & Kalogeraki, EM. **Handling of advanced persistent threats and complex incidents in healthcare, transportation and energy ICT infrastructures.** Evolving Systems (2020).

Die gute Nachricht ist, dass Unternehmen die Barriere der Komplexität deutlich, entschieden und effektiv überwinden können. Unter anderem darum soll es in diesem Whitepaper gehen. Aber bevor wir dazu kommen, werfen wir einen Blick auf die fünf größten Hindernisse für die erfolgreiche Bewältigung komplexer Vorfälle.

Die fünf Hindernisse für die erfolgreiche Bewältigung eines komplexen Vorfalls

Auch nachdem eine komplexe Bedrohung in eine Unternehmensumgebung eingedrungen ist, können Unternehmen diese aufhalten und mögliche Schäden eindämmen. Das fängt damit an, dass die Mehrzahl der

Erstzugangstaktiken innerhalb des MITRE ATT&CK Enterprise Frameworks immer noch relativ traditionell ist.

Dass allerdings Spear-Phishing selbst bei APTs noch immer zu den Einfallstoren gehört, sollte uns zu denken geben. Zum einen könnten sehr viele Angriffe durch die Automatisierung von Routineaufgaben schon im Vornherein wirksam abgewehrt werden. Zum anderen ist der Vorgang des Eindringens in den Unternehmensperimeter (mit Ausnahme zum Beispiel von Zero-Day-Exploits) nicht das, was einen Vorfall *komplex* macht.

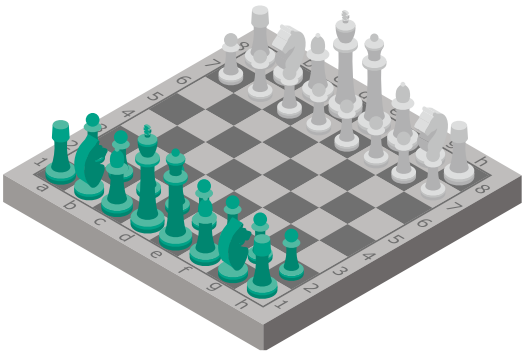
Die Komplexität beginnt mit Taktiken wie der horizontalen Infiltrierung, dem Einrichten von Backdoors sowie unterschiedlichen Formen der Payload-Übertragung und Tarnung. Aber was hindert IT-Sicherheitsteams daran, ihr Können und ihre Expertise einzusetzen, damit aus einem Vorfall kein komplexer Vorfall wird? Und wenn ein Vorfall komplex geworden ist, warum ist es dann oft so schwer, diesen einzudämmen und wirksam zu bekämpfen?

Hindernis Nr. 1: Die Komplexität der Cybersicherheitssysteme selbst

Für Außenstehende ist eine durchschnittliche Cybersicherheitskonfiguration ein Buch mit sieben Siegeln. So etwas wie ein durchschnittliches Großunternehmen oder eine durchschnittliche Cybersicherheitskonfiguration gibt es tatsächlich gar nicht. Man hat mehrere Tools für die unterschiedlichsten Spezialaufgaben, diverse Kontrollkonsolen und regelmäßige Warnmeldungen. Woher diese Komplexität stammt, haben wir bereits behandelt: Sie ist das Ergebnis einer stückweisen Reaktion auf die zunehmende Komplexität der IT-Sicherheitsinfrastruktur in Großunternehmen einerseits und der Bedrohungslandschaft andererseits.

Es ist deshalb fast schon eine Ironie des Schicksals, dass die Komplexität von Cybersicherheitskonfigurationen allzu oft zum Hindernis für die erfolgreiche Beseitigung genau der komplexen Vorfälle geworden ist, die sie eigentlich bekämpfen sollen. Dass die Komplexität eine erfolgreiche Eindämmung und Beseitigung verhindert, hat folgende Gründe:

- Aufgrund der Menge verschiedener Tools müssen Teams quasi die Rolle des „Dolmetschers“ übernehmen. Technologie-Stacks in der Cybersicherheit (und Technologie-Stacks im Allgemeinen) wirken oft wie eine Art virtueller Turm zu Babel – ein nahtloser, reibungsloser Betrieb scheitert an der Tatsache, dass jedes Tool seine eigene „Sprache“ spricht.
- Werden Vorfallsdaten in kleinen Stichproben aus einer Vielzahl unzusammenhängender Datensensoren an potentiellen Penetrationspunkten gesammelt, verlieren Teams häufig den Überblick und erkennen viel zu spät, dass ein komplexer Vorfall schon im Gang ist. Mit anderen Worten: Der Vorfall wird nicht richtig eingeschätzt, was schwere Schäden zur Folge haben kann.
- Die ständige manuelle Nacharbeit, die aus der unsystematischen und nicht konsistenten Vorfallsbehandlung resultiert, kostet so viel Energie, dass wichtige Alarme übersehen werden und man zu viel Zeit mit Fehlalarmen verbringt.



Hindernis Nr. 2: Schlechte oder irrelevante Threat Intelligence

Threat Intelligence muss einen dreistufigen Härtetest bestehen, wenn sie ihrem Anspruch gerecht werden soll, tiefe Einblicke in Cyberbedrohungen für Ihr Unternehmen zu liefern:

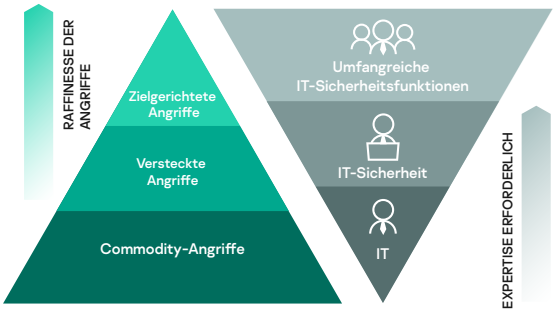
- Ist sie umfassend?
- Ist sie präzise?
- Ist sie aktuell?

Aber dieser Test ist nur der erste Schritt. Das wesentliche Hindernis für Großunternehmen besteht darin, dass sie zwar Zugang zu umfassender, präziser und aktueller Threat Intelligence haben, ihnen aber ein entscheidendes Puzzleteil fehlt: Relevanz. Jeder IT-Sicherheitsexperte, der mit den aktuell verfügbaren Threat Intelligence-Feeds vertraut ist, kennt dieses Problem nur allzu gut.

Relevanz als „Qualität statt Quantität" zu beschreiben, greift aber zu kurz. Threat Intelligence muss von einer Quelle stammen, die beides bietet. Darüber hinaus muss sie durch ein ganzheitliches Cybersicherheitssystem aufbereitet werden, um die für eine bestimmte Organisation, einen bestimmten Moment und eine bestimmte Umgebung relevanten Daten herauszufiltern. Die Ermittlung der Relevanz ist dabei als stetiger Prozess zu verstehen, der wie ein Regelkreis zwischen integrierten Elementen innerhalb einer geschlossenen Cybersicherheitskonfiguration funktioniert.

Threat Intelligence, die in relevanten Kontext und andere Erkennungs- und Threat Hunting-Mechanismen eingebettet ist, spart Zeit und schafft Klarheit, weil sie die Interpretation der Daten automatisch mitliefert.

Hindernis Nr. 3: Historisch bedingte, übermäßige Fokussierung auf einfache Commodity-Bedrohungen

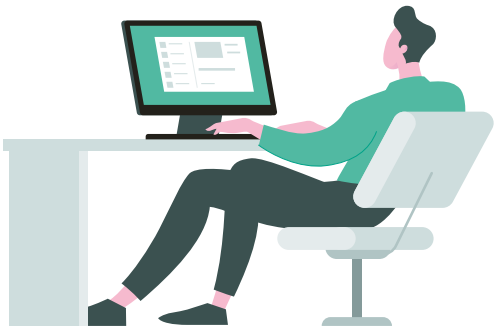


Einfache Commodity-Bedrohungen machen immer noch einen hohen Anteil aller Bedrohungen aus, mit denen Unternehmen konfrontiert sind. Deshalb ist es nicht verwunderlich, dass man selbst in großen Organisationen mit hohem IT-Reifegrad noch immer sehr stark auf diese Art von Bedrohung fokussiert ist.

Allerdings sind die Kosten im Zusammenhang mit diesen Bedrohungen vernachlässigbar im Vergleich zum potentiellen Schaden, den der verbleibende Prozentsatz verursacht – komplexe Übergriffe wie APT- und zielgerichtete Angriffe.

Ein weiterer Grund für die Fokussierung auf einfache Bedrohungen (zu Lasten komplexer Vorfälle) ist offensichtlicher. Es ist menschlich, sich auf ein überschaubares Problem zu konzentrieren, das leicht zu lösen ist. Einfache Bedrohungen werden selbst von einer rudimentären, schwach aufgestellten Cybersicherheitskonfiguration noch automatisch erkannt, auch wenn die Automatisierung nicht ausreicht, um sie zu beseitigen. So nehmen einfache Bedrohungen zu viel Raum ein, was zu Lasten einer Fokussierung auf komplexe Vorfälle geht, die weitaus gefährlicher sind.

Hindernis Nr. 4: Mangel an Cybersicherheits-ressourcen



Ein kurzer Blick auf die Cyberseek Heat Map, eine Initiative der US-amerikanischen National Initiative for Cybersecurity Education (NICE), zeigt das Ausmaß des Fachkräftemangels im Bereich Cybersicherheit. Obwohl sich Cyberseek ausschließlich auf den amerikanischen Kontext beschränkt, liefert sie einen sehr nützlichen (und ernüchternden) Einblick in die globale Situation.

Zum 30. Januar 2021 gab es in den USA 521.617 offene Stellen für Fachkräfte, bei gerade einmal 941.904 aktuell in der Cybersicherheit Beschäftigten. Das entspricht einem nationalen Verhältnis von Angebot zu Nachfrage von 1,8.

Beschäftigte in der Cybersicherheit wird das freuen, ihre Arbeitsplätze scheinen gesichert. Für die Qualität und Effizienz des Arbeitslebens sind das allerdings keineswegs gute Nachrichten.

Die meisten Analysten kommen zu dem Schluss, dass der Fachkräftemangel in der Cybersicherheit auf Versäumnisse in der Aus- und Weiterbildung zurückzuführen sind. Das hilft den betroffenen Unternehmen aber auch nicht. Bis der Fachkräftemangel beseitigt ist, müssen Organisationen die Leistung ihrer bestehenden IT-Sicherheitsteams optimieren und ihnen die Tools, den Support, die Rückendeckung und die Unterstützung, die sie brauchen, zur Verfügung stellen.

Hindernis Nr. 5: Reaktionsschnelle als Problem

Dieses letztes Hindernis für eine erfolgreiche Beilegung komplexer Vorfälle bildet das Bindeglied für die vier vorangegangenen. Angesichts komplexer Herausforderungen wie Zero-Day-Exploits, nicht auf Malware beruhenden, dateilosen oder LOTL-Angriffen (Living off the land) muss man vor allem schnell sein.

Ein komplexer Vorfall beginnt nicht zwangsläufig auf komplexe Weise, wie wir am Beispiel des Spear-Phishing als Taktik für den Erstzugang gesehen haben. Man könnte die teuren Folgen komplexer Vorfälle vermeiden, wenn das betreffende Team nur schnell genug reagieren könnte.

Das soll nicht heißen, dass es innerhalb der Entwicklung eines komplexen Vorfalls einen Punkt gibt, an dem „alles zu spät ist". Aber der Grad der Komplexität nimmt mit der Dauer zu. Man macht es sich aber auch zu leicht, wenn man bei komplexen Vorfällen nur auf Schnelligkeit setzt. Es sei denn, man interpretiert den Begriff des Schnellseins ein bisschen anders.

Schnell zu sein, bedeutet nicht, ständig im Notfallmodus zu sein oder sich auf jeden Warnhinweis zu stürzen. Schnellsein bedeutet, präzise, konsequent und entschieden alle wesentlichen Erkennungs- und Abwehrprozesse in Gang zu setzen. Dazu gehören unter anderem vorausschauendes Threat Hunting, Ursachenforschung und nachträgliche Analyse, Beseitigung, Eindämmung und Vorfallsreaktion.

Womit müssen Organisationen, die komplexen Vorfällen ausgesetzt sind, in der Zukunft rechnen?

Die ersten Monate des Jahres 2021 sind ein denkbar ungünstiger Moment, um Antworten auf Zukunftsfragen zu geben. Denn die Pandemie für sich gesehen, ist schon ein komplexer Vorfall, für den unsere Tools, Systeme und Experten nicht gerüstet waren. Aber einiges können wir trotzdem sagen. Wir wissen zum Beispiel, dass sich APTs und andere komplexe Angriffe weiterentwickeln werden. Und wir wissen, dass sich der Trend zum Homeoffice vermutlich über die Pandemie hinaus fortsetzen wird. Unser Global Research & Analysis Team (GReAT) hat die folgenden Vorhersagen für APTs im Jahr 2021 getroffen:

- Angriffe „unter falscher Flagge“ (wie Olympic Destroyer) werden ein neues Niveau erreichen
- Ransomware wird immer gezielter
- Es wird neue Online-Banking- und Zahlungsvektoren geben
- Es wird vermehrt Infrastruktur-Angriffe sowie Angriffe gegen Ziele geben, die keine PCs sind
- Mehr Angriffe in Regionen entlang den Handelsrouten zwischen Asien und Europa
- Zunehmende Verfeinerung der Angriffsmethoden
- Weitere Verlagerung in Richtung mobile Angriffe
- Missbrauch von personenbezogenen Daten: von Deep Fakes zu DNA-Lecks

Die Aussicht auf derartige komplexe Vorfälle muss uns aber nicht in Weltuntergangsstimmung versetzen.

Im ENISA-Bericht zu Forschungsthemen von Januar 2019 bis April 2020 erkennen wir einen Hoffnungsschimmer in dem Bereich, auf den wir uns bei der erfolgreichen Beilegung komplexer Vorfälle konzentrieren sollten: die menschliche Dimension. Darin heißt es:

„Cybersicherheit wird nach wie vor als eine Vorgehensweise zum Schutz von Netzwerken, Informationssystemen und Daten (NIS) gesehen. Diese Definition muss über die rein technischen Fragestellungen hinaus auf soziale, verhaltensorientierte und wirtschaftliche Belange sowie die unterschiedlichen Rollen aller Beteiligten erweitert werden. Dem sollte in künftigen Diskussionen um Forschung und Innovation im Bereich der Cybersicherheit Priorität eingeräumt werden. Ein besseres Verständnis der menschlichen Dimension ist der Schlüssel zur Entwicklung einer Cybersicherheitsstrategie, damit Sicherheitsentscheidungen getroffen werden, die den Bedürfnissen, Fähigkeiten und Erwartungen der Menschen gerecht werden.“

In dem für uns relevanten Bereich sind mit den oben genannten „Beteiligten“ die IT-Sicherheitsexperten sowie die Verantwortlichen in den Unternehmen gemeint. Wir werden vermutlich nicht zusätzliche Fachkräfte rekrutieren können. Deshalb muss die Frage lauten: Wie unterstützen wir die Mitarbeiter, die wir schon haben?

Technologien für Experten von Experten

Der erste Schritt besteht darin, sich klar zu machen, dass selbst Organisationen mit sehr hohem IT-Reifegrad komplexe Bedrohungen und APT-ähnliche Angriffe nicht im Alleingang bewältigen können. Es handelt sich um ein globales Problem, das immer wieder andere Regionen und Branchen betrifft. Zu viele Teams werden aus den in diesem Whitepaper vorgestellten Gründen daran gehindert, komplexe Vorfälle erfolgreich abzuwehren.

Deshalb möchten wir alle unsere Unternehmenskunden ermutigen, sich mit der Umsetzung der drei Säulen einer erfolgreichen Sicherheitsstrategie gegen komplexe Vorfälle zu befassen. Für IT-Sicherheitsteams sind das die folgenden drei Elemente:

- **Gut ausgestattet:**
  Cybersicherheit ist der eine Bereich, in dem selbst qualifizierte Mitarbeiter ihren Tools die Schuld zuschieben können. Für den effektiven Schutz vor Multi-Vektor-Angriffen und komplexen Vorfällen braucht man eine konsolidierte Plattform, die vollständige Transparenz schafft, störende Silos beseitigt, „Alarmermüdung" verhindert und Routineaufgaben innerhalb der Vorfallsreaktion übernimmt.

- **Fundiert:**
  Das vorhandene weitreichende Fachwissen in Organisationen mit hohem IT-Reifegrad darf niemals als Selbstverständlichkeit angesehen werden. Denn die Bedrohungslage verschiebt und wandelt sich ständig. Kontinuierliche Weiterbildung und leistungsstarke Threat Intelligence von einem zuverlässigen Cybersicherheitspartner sind entscheidend.

- **Bestärkt:**
  Wenn ein komplexer Vorfall oder APT aufgespürt wird, sollten selbst die besten IT-Sicherheitsanalysten auf Unterstützung von außen zurückgreifen können – in Form von Hintergrundinformationen, Bewertung der Sicherheitslage, Managed Threat Hunting und Incident Response. Denn obwohl komplexe Vorfälle, die aus APTs resultieren, in der Regel sehr zielgerichtet sind, haben sie selten nur ein Opfer im Visier. Externe Expertise kann helfen, branchenübergreifend und global den wahrscheinlichsten Ausbreitungspfad eines APT vorherzusagen, damit die Bedrohung mit sofort umsetzbaren Maßnahmen aus dem System entfernt werden kann.

Optimieren Sie die Arbeitsweise Ihrer IT-Sicherheitsexperten bei der Bearbeitung komplexer Vorfälle.

Optimieren Sie die Arbeitsweise Ihrer IT-Sicherheitsexperten bei der Bearbeitung komplexer Vorfälle mit Kaspersky Expert Security – ein umfassendes Abwehrkonzept, das Ihr Team auf dem Laufenden hält und bei der Abwehr besonders raffinierter und gezielter Cyberangriffe unterstützt. Die Extended Detection and Response-Plattform (XDR) umfasst eine ideal abgestimmte Kombination aus branchenführender Technologie, erstklassiger Threat Intelligence, menschlicher Expertise, Training und Services - unterstützt von den klügsten Köpfen der Branche. Unser ganzheitlicher Ansatz stärkt die Schlagkraft Ihres Cybersicherheitsteams bei der multidimensionalen Bedrohungserkennung, effektiven Untersuchungen und proaktivem Threat Hunting. Und er bietet schnelle, zentral gesteuerte Abwehrmaßnahmen gegen das gesamte Spektrum an modernen Bedrohungen

Weitere Informationen finden Sie hier: go.kaspersky.com/expert-de

Neues über Cyberbedrohungen: https://de.securelist.com/
IT Security News: www.kaspersky.de/blog
Threat Intelligence-Portal: opentip.kaspersky.de
Technologien im Überblick: www.kaspersky.com/TechnoWiki
Awards und Auszeichnungen: media.kaspersky.com/en/awards
Interaktives Portfolio-Tool: kaspersky.com/int_portfolio

www.kaspersky.de

kaspersky BRING ON THE FUTURE