Enttarnen moderner Bedrohungen

Cybersicherheit im Zeitalter dateiloser Bedrohungen, zielgerichteter Angriffe und APTs

kaspersky BRING ON THE FUTURE

Einleitung

Kurzer Rückblick: Verbrechen vor der Cyberkriminalität

In den Morgenstunden des 8. August 1963 überfiel eine Diebesbande den Zug der Royal Mail und stahl 120 mit Geldscheinen gefüllte Säcke – in einem Wert von insgesamt sieben Millionen US-Dollar (nach heutigem Wert ca. 50 Millionen). Dieser Raub hat die Fantasie von Menschen auf der ganzen Welt angeregt, die aus den Dieben (Anti-)Helden machten. Die Folge waren Filme, Serien, Bücher, Songs und sogar Videospiele (einschließlich einer Quest in **Runescape**) über die Verbrecher. Alle 15 Beteiligten bis auf vier wurden gefunden, verhaftet und verurteilt.

Der legendäre Postzugraub:
50 Millionen USD (nach heutigem Wert)

NotPetya-Angriff (2017 bis ...):
10 Milliarden USD

Cyberkriminalität lässt alte Verbrechen verblassen

Am 27. Juni 2017 gaben Forscher des Kaspersky Global Research and Analysis Team (GReAT) eine Ransomware-ähnliche Wiper-Attacke bekannt, die sich **NotPetya** nannte, um sich so von den 2016er Petya-Varianten zu unterscheiden. Der Angriff nutzte einen EternalBlue-Exploit, um sich in Unternehmensnetzwerken zu verbreiten. Der Gesamtschaden der NotPetya-Attacke wird auf 10 Milliarden US-Dollar geschätzt. Bei manchen Opfern erreichen die Schäden mehrere Hundert Millionen. Merck verlor insgesamt 870 Millionen US-Dollar, FedEx 400 Millionen und Maersk 300 Millionen. Zum Zeitpunkt dieses Whitepapers ist in diesem Fall erst eine Festnahme erfolgt.

Cyberkriminalität: das ultimative Verbrechen aus der Ferne

Kriminelle müssen heute keine Züge mehr anhalten. Sie können verheerende (und äußerst rentable Angriffe) bequem von ihrem Schreibtisch aus planen und ausführen.

Bei Cyberverbrechen sind deshalb deutlich weniger Spuren am „Tatort“ zu finden als bei physischen. Von Indizien wie Fingerabdrücken können Experten der Cyberforensik nur träumen. Und auch der Tatort selbst ist nur schwer zu ermitteln. Denn Cyberangriffe überwinden nationale Grenzen und brechen still und leise in die IT-Umgebungen von Unternehmen ein.

Verwischte Spuren

Im Zeitraum zwischen Postzugraub und NotPetya hat sich Kriminalität stark weiterentwickelt, wenn es darum geht, Spuren zu verwischen und Verbrechen aus immer größerer Entfernung durchzuführen. Doch diese Entwicklung ist noch längst nicht vorbei. In einigen Jahren ist die von den NotPetya-Angreifern eingesetzte Technologie möglicherweise schon wieder veraltet – so wie es der Postzugraub heute ist.

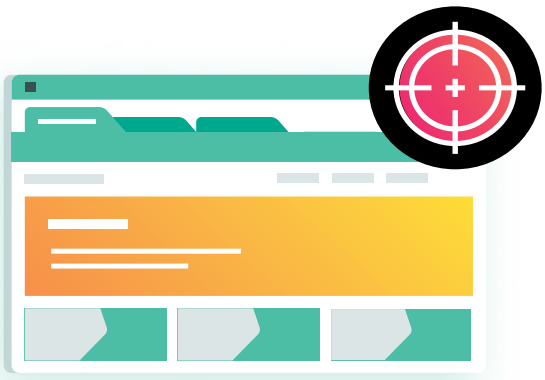
Neue Tarnmethoden

In diesem Whitepaper behandeln wir einige Aspekte neuer Tarnmethoden, darunter die zunehmende Entwicklung cyberkrimineller Techniken, die es Verbrechern ermöglichen, die Verteidigung klassischer Cybersicherheitslösungen zu durchdringen und nahezu ohne forensische Indizien verheerende Schäden anzurichten. Darüber hinaus stellen wir einige leistungsstarke (und einfache) Möglichkeiten vor, wie Sie Ihr Unternehmen effektiv vor schwer auffindbaren Angriffen schützen können – ganz ohne Zusatzaufwand für Ihr Team und trotz des anhaltenden Mangels an Cybersicherheitsressourcen.

Die Anatomie zielgerichteter Angriffe

Gezielte Attacken sind das Präzisionswerkzeug unter modernen getarnten Bedrohungen: Angreifer suchen sich ihre Opfer genau aus und passen ihre Methoden im Detail an, um unzureichend geschützte Systeme (oder unachtsame Nutzer) auszunutzen und Unternehmen so in die Knie zu zwingen. Eingesetzte Methoden und Charakteristiken umfassen:

- Cyberkriminelle untersuchen das Endpoint-Schutzsystem des Opfers, bevor sie einen Angriff starten, um einen passenden Mechanismus zu entwickeln, der das System automatisch umgeht.
- Zero-Day-Schwachstellen und unkompromittierte Nutzerkonten, über die unzureichend geschützte Unternehmen aus dem Nichts angegriffen werden
- Maßgeschneiderte Schadsoftware, die nur zur Schädigung eines bestimmten Unternehmens entwickelt wurde
- Kompromittierte Konten, die normal scheinen, und Umgehung unzureichender Endpoint-Schutzlösungen bzw. Ausnutzung fehlender Endpoint Detection and Response
- Multi-Vektor-Angriffe, bei denen gleichzeitig so viele Endpoints wie möglich angegriffen werden
- Ausgeklügeltes **Social Engineering** und Angriffe, die auf spezifischen und persönlichen Insiderdaten basieren und oft auf die Führungsebene abzielen



False Positives – die Flut falscher Flags

False Positive-Raten reichen von 30 bis hin zu 99 Prozent. Dieses Problem hat zwei Seiten. Einerseits führen Fehlalarme zu Belastung: Das IT-Team verschwendet kostbare Stunden mit der Untersuchung jedes Alarms, sodass True Positives der potentiell unzureichenden Cyberabwehr entgehen. Andererseits führen hohe False Positive-Raten dazu, dass IT-Mitarbeiter die oben beschriebene Belastung ausgleichen, indem sie die Empfindlichkeit ihrer Cybersicherheitslösungen reduzieren, damit weniger Alarme auftreten. In beiden Fällen können False Positives schwere Folgen haben.

Die gute Nachricht ist, dass Sie False Positives vollständig beseitigen und sich nur auf relevante Bedrohungen konzentrieren können. Als **AV-Test** Kaspersky Endpoint Security for Business getestet hat (neben den Endpoint-Schutzlösungen von 14 weiteren Anbietern), erzielte unser Produkt bei Erkennung und Blockierung eine False Positive-Rate von Null.

Dateilose Bedrohungen

Cyberkriminelle nutzen vermehrt dateilose Angriffe. Das stellt vor allem Unternehmen, die sich in der Vergangenheit ausschließlich auf klassische Endpoint-Schutzlösungen verlassen haben, vor neue Herausforderungen.

Am Tag nach unserer Bekanntgabe des NotPetya-Angriffs haben wir Unternehmen auf der ganzen Welt dazu beraten, wie sie sich schützen können. Dies beinhaltete klare Anweisungen, mittels der Programmkontrolle von Kaspersky Endpoint Security for Business die Ausführung der Datei perfc.dat zu unterbinden. Für dateilose Angriffe ist eine solche Anweisung nicht möglich. Hier braucht es einen neuen Ansatz, den wir weiter unten vorstellen.

Bei dateilosen Attacken kommen unter anderem folgende Methoden zum Einsatz:

- **Schädliche Skripte, die in WMI-Konten gespeichert werden**
- **Schädliche Skripte, die direkt als Befehlszeilenparameter an PowerShell übergeben werden**
- **Schädliche Skripte, die in der Registrierung und/oder im Taskplaner des Betriebssystems gespeichert werden**
- **Schädliche Programmdateien, die direkt in den Arbeitsspeicher extrahiert und dort ausgeführt werden, ohne zuvor auf der Festplatte gespeichert zu werden – mittels Reflexion in .Net**

Aufgrund ihrer Unauffälligkeit sind dateilose Angriffe zehnmal häufiger erfolgreich als dateibasierte. Eine der bekanntesten dateilosen Attacken war der Vorfall bei der amerikanischen Kreditagentur Equifax 2017, die zum Diebstahl von 146,6 Millionen Kundendatensätzen führte.

Kaspersky Endpoint Security for Business analysiert Verhalten, nicht nur Dateien

Wenn es keine verdächtige Datei gibt, die gefunden werden kann, lassen sich Angriffe nur über die Erkennung verdächtigen Verhaltens ermitteln. Dateilose Angriffe ohne eine solche Verhaltensüberwachung verhindern zu wollen, ist ein absolut hoffnungsloses Unterfangen.

Die Kaspersky-Technologie zur Verhaltenserkennung nutzt laufend proaktive Machine Learning-Prozesse, unterstützt durch die umfangreiche Threat Intelligence, die das Kaspersky Security Network mittels Data Science-Verarbeitung und Analyse globaler Echtzeitstatistiken gewinnt.

Unsere Exploit Prevention-Technologie blockiert Malware, die versucht, Software-Schwachstellen auszunutzen. Gleichzeitig kann Adaptive Anomaly Control Aktionen blockieren, die vom aufgezeichneten Muster abweichen (z. B. um den Start von PowerShell zu verhindern).

Der Mangel an Cybersicher-heitsressourcen

Neben immer unauffälligeren Angriffen haben Unternehmen auch mit einem anhaltenden Mangel an Cybersicherheitsressourcen zu kämpfen. Cyberkriminelle verbessern sich stetig, doch Cybersicherheitsexperten, die in der Lage sind, es mit diesen Kriminellen aufzunehmen, sind rar auf dem Arbeitsmarkt. Sie zu gewinnen und zu halten, stellt daher eine echte Herausforderung dar.

2019 hieß es im **Forbes Magazine**, dass „nicht gefüllte Cybersicherheitsstellen bis 2022 die 1,8-Millionen-Marke erreichen werden – ein Anstieg von 20 Prozent gegenüber den 1,5 Millionen aus 2015". Das **Security Magazine** war noch etwas deutlicher: „Es herrscht ein Krieg um Cybersicherheitsexperten."

Leider haben schon zu viele Unternehmen – nachdem sie endlich einen internen IT-Sicherheitsexperten gefunden, angestellt und geschult hatten – miterleben müssen, wie dieser Experte das Unternehmen verlässt und seine unbezahlbare Expertise bei anderen Unternehmen einsetzt – für ein höheres Gehalt.

Doch auch abseits des Talentmangels sind interne Vollzeit-Cybersicherheitsexperten oft nur schwer mit dem Budget vereinbar – gerade in Unternehmen, die schon jetzt kaum die IT-Ressourcen aufbringen können, die sie für eine erfolgreiche digitale Transformation benötigen.

Bis der Mangel an Cybersicherheitsressourcen vorüber ist, lässt sich zukunftssichere Cybersicherheit im Rahmen beschränkter Budgets und Skills nur über Technologie erreichen. Menschliche Expertise ist zwar weiterhin essentiell, doch die richtige IT-Sicherheitstechnologie kann als wichtige Verbindung zwischen überlasteten IT-Teams und branchenführender Sicherheitsanalyse dienen.

Bei uns erfolgt diese Verbindung zwischen IT und Sicherheitsanalyse über Kaspersky Sandbox: Die Lösung blockiert automatisch komplexe Bedrohungen auf Workstation- und Serverebene. Bei der Entwicklung von Kaspersky Sandbox wollten wir vor allem IT-Teams entlasten, damit sie sich auf die Verwaltung anderer notwendiger Aufgaben konzentrieren können.

Und genau dieses Ziel erreicht die Kaspersky Sandbox: Kleine Unternehmen können moderne Bedrohungen abwehren, ohne IT-Sicherheitsexperten in Vollzeit anzustellen, während größere Unternehmen den Aufwand ihrer internen Experten und die zugehörigen Kosten deutlich reduzieren können, indem sie die meisten Aufgaben für fortschrittlichen Bedrohungsschutz automatisieren, darunter auch Priorisierung und Analyse.

Basierend auf einer dynamischen Bedrohungsemulation (Sandbox-Technologie) nutzt Kaspersky Sandbox die Best Practices unserer Experten für die Abwehr komplexer Bedrohungen und APTs und ist eng in Kaspersky Endpoint Security for Business integriert. Und so funktioniert die Lösung:

- Kaspersky Endpoint Security for Business sendet eine Scananfrage für ein bestimmtes Objekt an die Kaspersky Sandbox.
- Kaspersky Sandbox führt den Scan in einer Umgebung durch, die von der echten Unternehmensinfrastruktur isoliert ist. Hierzu werden virtuelle Maschinen eingesetzt, die über verschiedene Tools eine normale Arbeitsumgebung simulieren.
- Kaspersky Sandbox erfasst und analysiert Artefakte und nutzt Verhaltensanalysen.
- Wenn ein Objekt eine schädliche Aktion durchführt, erkennt die Kaspersky Sandbox es als schädlich und weist ihm eine entsprechende Bewertung zu.
- Abhängig von dem Ergebnis blockiert Kaspersky Endpoint Security for Business die Datei entweder automatisch oder markiert sie als sicher.
- Das Ergebnis wird in Echtzeit an den gemeinsamen Speicher gesendet, damit auch andere Hosts mit Kaspersky Endpoint Security for Business schnell Informationen zum gescannten Objekt abrufen können, ohne die Datei erneut analysieren zu müssen.

Die Kaspersky Sandbox ist schnell, dynamisch und effizient und ermöglicht Unternehmen weltweit den Zugang zu komplexer IT-Sicherheitsexpertise. Dank der engen Integration in Kaspersky Endpoint Security for Business bietet die Kaspersky Sandbox eine essentielle Verteidigung gegen komplexe moderne Bedrohungen – selbst für Unternehmen, die noch nicht über interne IT-Sicherheitsexperten verfügen.

Horizontale Infiltrierung von APTs

Altmodische Malware-Angriffe verhielten sich ganz ähnlich wie die Diebe des Postzugraubs: Sie drangen in ein System ein, nahmen, was sie wollten, und flüchteten, so schnell sie konnten. Doch im Zeitalter unauffälliger Bedrohungen haben sich nicht nur die Ziele, sondern auch die Methoden von Cyberkriminellen verlagert.

Horizontale Infiltrierung von Malware ist ein wichtiger Faktor für die Hartnäckigkeit von Advanced Persistent Threats (APTs). Anstatt einzudringen und sich sofort wieder zurückzuziehen, nutzen Cyberkriminelle verschiedenste Tools, um sich im angegriffenen System auszubreiten, indem sie von Gerät zu Gerät springen. Solche Angriffe können eine dauerhafte Kompromittierung verursachen, bei der Opfer scheinbar endlosen schädlichen Vorfällen ausgesetzt sind.

Horizontale Infiltrierung liegt jetzt schon im Trend und wird immer beliebter. In unserem **jährlichen APT-Bericht für 2019** haben wir vor zwei APTs gewarnt, die in jüngster Vergangenheit Methoden zur horizontalen Infiltrierung eingesetzt haben:

- Neue Aktivität von BlueNoroff, bei der sich Angreifer über eine öffentliche Liste mit Anmeldedaten und eigens entwickelte PowerShell-Skripte im Netzwerk ausbreiten, um auf wertvolle Hosts zuzugreifen
- Horizontale Infiltrierung durch Icefog-Bedrohung, bei der eine Methode namens Load Order Hijacking zum Einsatz kommt

„Angesichts der gesteigerten Komplexität und Häufigkeit von Cyberattacken werden Angriffserkennung und Vorfallsreaktion immer wichtiger."

Gartner, Inc.

Abwehr von APTs mit Transparenz, Analysen und Einblicken

Um die Hartnäckigkeit von APTs zu beseitigen und horizontale Infiltrierung zu verhindern, sind sehr spezifische EDR-Funktionen (Endpoint Detection and Response) erforderlich, die sich in zwei Kategorien unterteilen lassen: Transparenz und Analyse.

- **Transparenz**
  - Die Fähigkeit, über eine zentrale Oberfläche alle Endpoints gleichzeitig in Echtzeit zu visualisieren und zu überwachen
  - Kontextinformationen zur individuellen Endpoint-Aktivität sowie Prozesse, Zeitverläufe und Korrelationen zwischen Endpoints im gesamten Unternehmen
  - Erfassung kostbarer Sicherheitsinformationen zur weiteren Untersuchung und Reaktion durch einen IT-Sicherheitsexperten

Ohne EDR reichen die Kosten für das System-Reimaging (zur effektiven Wiederherstellung funktionierender Zustände) im Falle eines Vorfalls von 400 bis 600 US-Dollar pro Vorfall.

— **Analyse**
  - **Integrierte Zuordnung und Korrelation verschiedener Ergebnisse aus unterschiedlichen Erkennungsmechanismen, die in einem einheitlichen Vorfall zusammengeführt werden, um Taktik, Prozesse und Methoden der Bedrohung zu verstehen**
  - **Rückblickende Analyse zur horizontalen Infiltrierung**
  - **Analyse von Ereignissen, die in der „Grauzone“ zwischen vertrauenswürdigen/legitimen Objekten und Prozessen stattfinden, sowie von Ereignissen, die eindeutig schädlich sind, darunter:**
    - Zero-Day-Schwachstellen
    - Eindeutige Schadsoftware (bisher noch nicht aufgetreten)
    - Neue/unbekannte Malware
    - Kompromittierte legitime Software/Prozesse

„Nutzen Sie die EDR-Module, die bei Ihrem EPP-Anbieter verfügbar sind.“

Gartner, Inc.: Endpoint Detection and Response Architecture and Operations Practices

Ohne EDR schießen die Kosten für die Erfassung und Analyse von Indizien von Hunderten verschiedenen Endpoints und Systemen für die Vorfallsreaktion schnell in die Höhe – manche Sicherheitsexperten berechnen hier 600 US-Dollar pro Stunde.

Ein kurzes Wort zum Mythos der Cybersicherheit von macOS

macOS-Geräte verdienen es, hier speziell erwähnt zu werden – und zwar wegen des gefährlichen Mythos, dass ihr Betriebssystem auf wundersame Weise immun gegen Cyberangriffe ist. Der einzige Grund dafür, dass macOS-Geräte seltener Cyberangriffen zum Opfer fallen, ist, dass es weniger von ihnen gibt. Das führt dazu, dass Cyberkriminelle in der Regel eher auf das weiter verbreitete Betriebssystem (in der Regel Windows) abzielen. Früher waren macOS-Geräte nur bei Designern und anderen Kreativarbeitern zu finden, die in der Regel nur eingeschränkten Zugriff auf zentrale Systeme benötigen. Heute jedoch werden sie immer beliebter, insbesondere bei Start-ups und anderen innovativen Unternehmen, die durch IT-Konsumerisierung beeinflusst werden. Dieser Begriff beschreibt das Phänomen, dass sich das IT-Verhalten von Verbrauchern auf Unternehmen auswirkt.

Cyberkriminelle richten ihre Aufmerksamkeit zunehmend auf Schwachstellen, die durch unzureichend geschützte macOS-Geräte entstehen. Im ersten Halbjahr 2019 haben wir **nahezu sechs Millionen Phishing-Angriffe erkannt**, die auf macOS-Nutzer abzielten – 11,8 Prozent davon auf Unternehmensnutzer. Darüber hinaus haben wir auch zwei Trojaner entdeckt, die es auf macOS-Nutzer abgesehen haben: Trojan.OSX.Spynion und Trojan-Downloader.OSX.Vidsler. Der erste enthält eine Backdoor, über die Angreifer sich remote mit dem macOS eines Nutzers verbinden können, und wird über verschiedene kostenlose macOS-Programme verbreitet. Der zweite wird hingegen über Links in Bannerwerbung verteilt.

Gerätechaos: moderne Bedrohungen, gemischte Umgebungen und BYOD

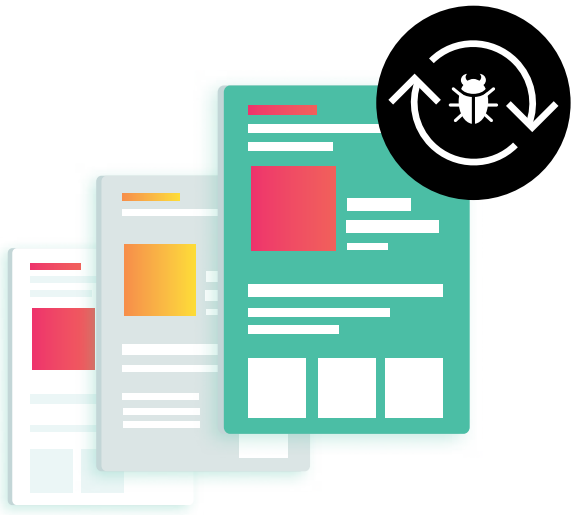
Für den Aufbau der perfekten IT-Umgebung braucht es zahlreiche Geräte, Betriebssysteme, Netzwerkprotokolle und Technologien. Und da der BYOD-Trend (Bring Your Own Device) nicht abzubrechen scheint, ist die IT-Umgebung oftmals nicht nur stark gemischt, sondern unvorhersehbar.

Ein normales IT-Setup umfasst Windows und/oder Linux für Backend-Systeme, während die Büromitarbeiter mit Windows- oder macOS-Geräten arbeiten. Darüber hinaus wird die mobile Bereitstellung immer komplexer: Hier kommen oft spezielle Tablets oder andere Geräte für missionskritische Prozesse und Services zum Einsatz.

Im Zeitalter unauffälliger Bedrohungen stellen gemischte Umgebungen ein besonders beliebtes Ziel für Cyberkriminelle dar. Denn die Übersicht über die zahllosen verschiedenen Technologien und Geräte zu behalten, ist eine echte Herausforderung für die IT. So kommt es häufig zu Rissen in der Unternehmensverteidigung. In einer hypervernetzten Welt reicht ein unzureichend geschützter Endpoint aus, um ins System einzudringen und die IT-Umgebung des Opfers wie oben beschrieben horizontal zu infiltrieren.

Dass Unternehmen in einer solchen Welt eine intuitive Lösung benötigen, über die sie ihre Cybersicherheit von überall aus bis ins kleinste Datei managen können, ist klar – doch bei gemischten Umgebungen reicht eine solche Lösung möglicherweise nicht mehr aus. Mit dem NEUEN Kaspersky Security Console Cloud gehen wir noch einen Schritt weiter und passen die Lösung an die gemischten Umgebungen unserer Kunden an – mit unserer individuellen Bereitstellung (und Upgrades).

Bei der NEUEN Kaspersky Security Console Cloud liegt der Fokus auf Geräten und Nutzern. Die Lösung bietet eine rollenbasierte Zugriffssteuerung (RBAC) sowie Unterstützung für Serverhierarchien. Das macht die Verwaltung von Kaspersky-Sicherheitsprogrammen für Windows, Linux und macOS zum Kinderspiel. Außerdem umfasst die Lösung Hypervisorfunktionen sowie eine zentral automatisierte Erkennung und Bereitstellung, um Risse in der Cyberverteidigung zu verhindern. Die Migration von lokalen Implementierungen der Kaspersky Security Console erfolgt ganz einfach über einen Assistenten, der verschiedene Optionen für stufenweise bzw. Übernahmemigrationen bietet (Letzteres via Einstellungsexport).



Das seltsame Verhältnis von Volumen zu Kosten

Die Flut einfacher Malware nimmt kein Ende: Cyberkriminelle bombardieren Unternehmen auf der ganzen Welt auch weiterhin mit Phishing-Angriffen, Viren, Trojanern und einfacher Spy- und Malware. Tatsächlich machen solche Attacken immer noch 90 Prozent aller Cyberangriffe aus.

Doch die starke Verbreitung einfacher Malware lenkt von einem wichtigen, aber oft missachteten Fakt ab: Die übrigen zehn Prozent der Attacken, unter denen auch APTs zu finden sind, kosten nahezu 100 Mal mehr pro Vorfall als einfache Malware. Die durchschnittlichen Kosten einfacher Vorfälle liegen bei 10 000 US-Dollar; die für einen APT-Vorfall bei 926 000.

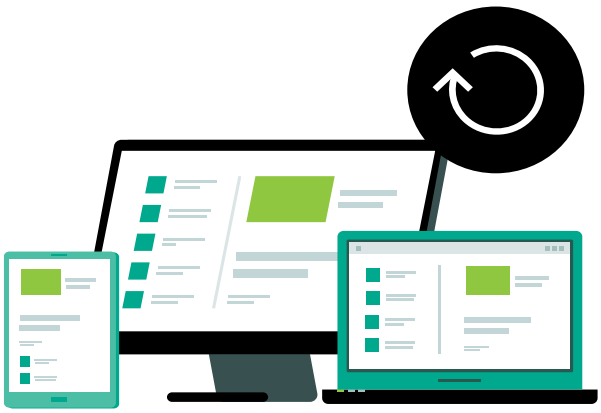
Die Situation lässt sich mit einem umgekehrten Eisbergmodell beschreiben: Die 90 Prozent sind oberhalb des Wasserspiegels und vollständig sichtbar, während die tödlichen zehn Prozent im Verborgenen liegen. Doch die gute Nachricht ist, dass wir die 90 Prozent nicht ignorieren müssen, um auch die tödlichen zehn in den Griff zu kriegen. Bei einem Test von **AV-Test** (Oktober 2019) hat Kaspersky Endpoint Protection for Business eine optimale Erkennungsrate von 100 Prozent bei dateilosen Bedrohungen sowie die höchste Verhinderungsrate unter 14 Anbietern (94,12 %) erreicht.

Die verborgenen zehn Prozent zu ignorieren, ist keine Option und die Kosten für Vorfallsreaktion und Wiederherstellung nach einem APT-Angriff sind finanziell verheerend – Kosten, die sich mit der richtigen Vorbereitung hätten vermeiden lassen.

Auch die Unterteilung des Bedrohungseisbergs in zwei (wenn auch ungleiche) Hälften ist nicht nötig. Tatsächlich ist diese Unterteilung im täglichen Sicherheitsbetrieb jedes Unternehmens überflüssig. Beide Bedrohungskategorien haben letztlich dasselbe Ziel – der Unterschied liegt nur in der Bösartigkeit der Methoden (und den daraus resultierenden Kosten und Schäden).

Sich nicht ausreichend vor den einfachen Bedrohungen zu schützen, die durch die 90 Prozent oberhalb der Wasseroberfläche dargestellt werden, kann das Unternehmen langfristig in die Knie zwingen. Selbst die einfachste Attacke kann Ressourcen belasten und mit der Zeit zermürben – gerade wenn IT-Budgets knapp und Cybersicherheitsexperten nur schwer zu finden und zu halten sind. Kaspersky Endpoint Security for Business entlastet die IT um den manuellen Kampf gegen zahlreiche dieser einfachen Bedrohungen. So können sich Unternehmen auf APTs und andere komplexe Angriffe konzentrieren. Gleichzeitig arbeitet die Kaspersky Sandbox nahtlos mit Kaspersky Endpoint Security for Business zusammen, um automatisch moderne und nur schwer auffindbare Bedrohungen zu blockieren.

Für die zehn Prozent unterhalb des Meeresspiegels ist Endpoint Detection and Response essentiell. Manche Unternehmen können sich nur schwer vorstellen, warum EDR in der heutigen Bedrohungslandschaft eine so tragende Rolle spielt. Doch wenn Sie bei einem Unternehmen nachfragen, das jüngst einem APT-Angriff zum Opfer gefallen ist, wird der Fall für EDR schnell klar: Lieber schon heute die Cyberabwehr optimieren, um ein sicheres und rentables Morgen zu gewährleisten.



„Ein integriertes Paket bietet Ihnen die Möglichkeit, EDR angemessen zu implementieren, zu betreiben und den nötigen Mehrwert daraus zu ziehen.“

Kuppinger Cole

Enge Integration bedeutetwasser-dichte Cyber-abwehr

Mit Kaspersky können Sie ganz einfach den gesamten Eisberg abdecken: Kaspersky Endpoint Detection and Response und Kaspersky Sandbox lassen sich nahtlos in Kaspersky Endpoint Protection for Business integrieren und alles wird über eine zentrale Oberfläche, Kaspersky Security Console Cloud, verwaltet – genauso, wie es sein sollte. Sie müssen weder zwischen unterschiedlichen Systemen hin- und herwechseln noch sich neue Prozesse für Softwaremanagement aneignen, was in der modernen Bedrohungslandschaft einen enormen Aufwand bedeuten würde.

Mit unseren in der Branche und bei Kunden bewährten Lösungen für Cybersicherheit mit EDR im Kern können Sie selbst schwer auffindbare Angriffe blitzschnell erkennen und abwehren – ganz ohne Zusatzaufwand für Ihr Team.

Um den anhaltenden Mangel an Cybersicherheitsressourcen auszugleichen, ermöglicht unser eng integriertes vorausschauendes Cyberabwehrsystem völlig mühelos messerscharfe Analysen. Dank Endpoint-Transparenz und automatisierter Priorisierung können Sie Ihre Aufmerksamkeit auf gefährlichere Bedrohungen wie zielgerichtete Angriffe richten.

Vielfach ausgezeichneter Endpoint-Schutz, eine automatisierte Sandbox und eine einheitliche Cloud-Konsole arbeiten Hand in Hand mit EDR, um Ihre gesamte IT-Umgebung optimal zu schützen.

Minimieren Sie noch heute die Risiken für künftiges Geschäftswachstum.

Neues über Cyberbedrohungen: https://de.securelist.com/
IT-Sicherheitsnachrichten: https://www.kaspersky.de/blog/b2b/

www.kaspersky.com

kaspersky BRING ON THE FUTURE