KASPERSKY lab

BEST PRACTICES

Kontrolltools

www.kaspersky.de

LEITFADEN ZU BEST PRACTICES FÜR KONTROLLTOOLS

Cyber-Spionage und staatlich sanktionierte Bedrohungen sind in der letzten Zeit immer wieder in den Schlagzeilen. Tatsache ist aber, dass die gleiche Technologie auch gegen Unternehmen wie Ihres eingesetzt werden kann und auch eingesetzt wird.

Sie können das Internet nicht einfach abstellen, und Sie können auch nicht alles im Blick haben, was in Echtzeit im Unternehmensnetzwerk vor sich geht. Sie haben aber die Möglichkeit, diese Aktivitäten zu verwalten und zu steuern. Insbesondere können Sie Maßnahmen ergreifen, wenn ihre Endbenutzer etwas unbedacht anklicken oder installieren. Hier erfahren Sie, wie dies möglich ist.

1. NICHT NUR BLOCKIEREN, SONDERN KONTROLLIEREN

Social Media, intelligente Geräte, Web-basierte Programme, Spam, Phishing, schädliche Webseiten, Social Engineering, Malware. Für IT-Manager ist es eine große Herausforderung, mit den zunehmend komplexen Bedrohungen Schritt zu halten, deren Angriffsmöglichkeiten sich immer mehr vermischen.

Und dabei geht es lediglich um die Risiken von außerhalb Ihres Unternehmens. Wie sieht es aber mit den Aktivitäten der Endbenutzer innerhalb des Unternehmens aus, die zu Sicherheitsverletzungen und Datenlecks führen? In Online-Spielen eingebetteter Schadcode, gefährliche Links in den Programmen für Soziale Netzwerke, in scheinbar harmlosen Office-Dokumenten versteckte Malware ... Die heutigen Cyberkriminellen nutzen Schwachstellen im Hinblick auf Einzelbenutzer aus, um Zugriff auf Unternehmensnetzwerke und die darauf gespeicherten vertraulichen Daten zu erlangen.

Mit Programm-, Geräte- und Web-Kontrollen sowie einer leistungsstarken Anti-Malware-Technologie können Sie Ihr Unternehmen schützen, ohne Einbußen bei Produktivität und Flexibilität hinnehmen zu müssen. Übernehmen Sie die Kontrolle über Ihre Unternehmenstechnologie, indem Sie diese einfach zu implementierenden Web-, Programm- und Gerätekontrollen einführen.

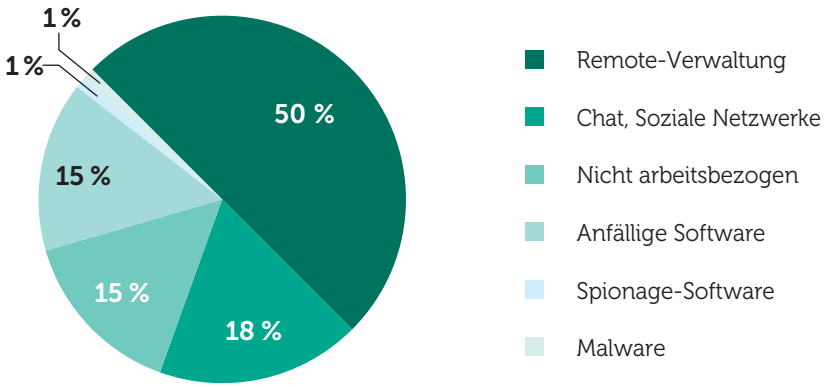
Achtung bei Software-Programmen

Schwachstellen in Webprogrammen sind in unserer extrem vernetzten Welt zu einem beliebten Ziel für Cyberkriminelle geworden. Allein im Jahr 2014 hat Kaspersky Lab mehr als **6,2** Milliarden, von globalen Online-Ressourcen ausgehende Angriffe entdeckt und neutralisiert[1], verglichen mit **1,7** Milliarden 2013[2].Diese Angriffe gingen von **9,7** Millionen unterschiedlichen Hostcomputern aus[3]. Kaspersky Lab erkennt täglich mehr als **325.000** neue schädliche Dateien[4].

Einer von **14** Downloads enthält heute eine Form von Malware[5]. Mit einem einfachen Blockieren von Downloads ist es daher nicht getan ... und jeden Tag setzen Kriminelle Malware ein, um Schwachstellen in legitimer Unternehmenssoftware auszunutzen: Programme von Drittanbietern machen durchschnittlich **75** Prozent aller Schwachstellen aus[6].

1 Kaspersky Security Bulletin, Dezember 2014
2 Kaspersky Security Bulletin, Dezember 2013
3 Kaspersky Security Bulletin, Dezember 2014
4 Kaspersky Security Bulletin, Dezember 2014
5 Kaspersky Security Bulletin, Dezember 2014
6 Secunia Vulnerability Review 2014

Tatsache für IT-Sicherheitsexperten ist es, dass sich das schwächste Glied in der Sicherheitskette oft bereits auf ihren Systemen befindet – oder ihnen direkt gegenüber sitzt.



2. PROGRAMMKONTROLLE UND WHITELISTING VERHINDERN VON BEDROHUNGEN UND SICHERHEITSVERLETZUNGEN

Programmkontrolle und dynamische Whitelist-Technologie ermöglichen den Schutz von Systemen vor bekannten und unbekannten Bedrohungen, da Administratoren unabhängig vom Endbenutzerverhalten umfassende Kontrolle über die Art von Programmen erhalten, die auf ihren Endpoints ausgeführt werden dürfen.

Im Grunde ermöglichen Programmkontrollen ein effizienteres Erstellen und Umsetzen von Sicherheits- und Nutzungsrichtlinien in Ihrem Unternehmen:

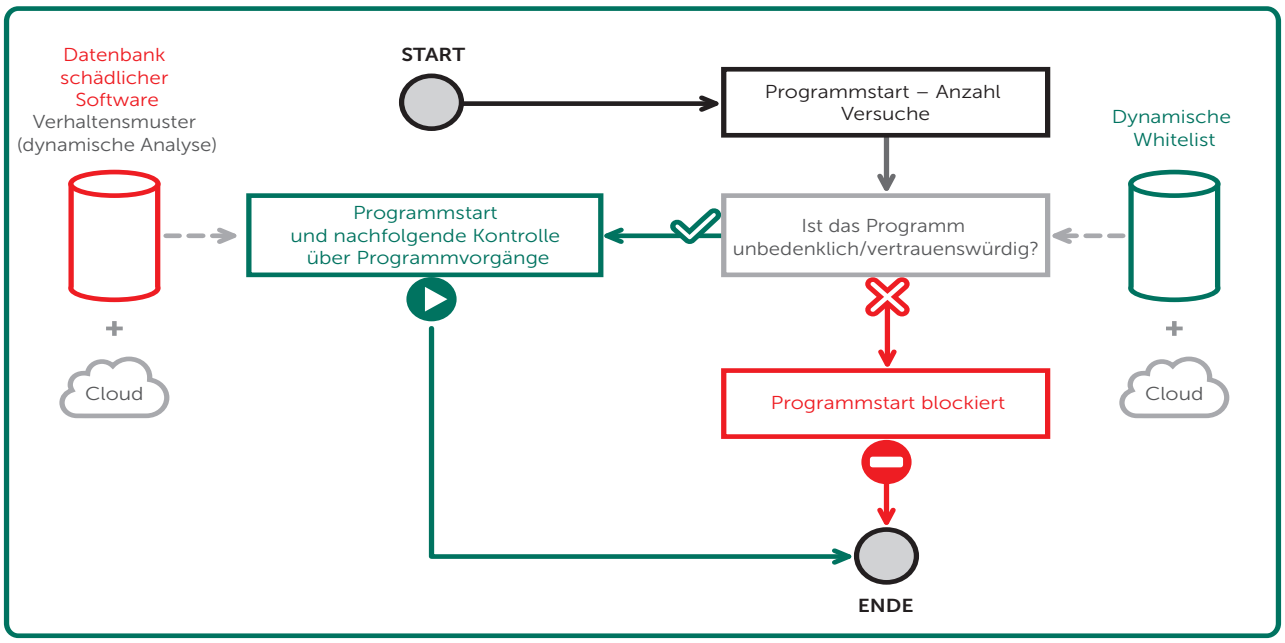
- **Programmstart-Kontrolle**: Programmstarts ausführen, blockieren und überprüfen. Ermöglicht Produktivitätssteigerungen durch Zugriffsbeschränkungen für nicht unternehmensrelevante Programme.
- **Kontrolle der Programmberechtigungen**: Reguliert und kontrolliert den Zugriff eines Programms auf Systemressourcen und Daten und klassifiziert Programme als vertrauenswürdig, nicht vertrauenswürdig oder eingeschränkt.
- **Vulnerability Scanning von Programmen**: Schnelle Abwehr von Angriffen auf Schwachstellen in vertrauenswürdigen Programmen.
- **Programmüberwachung**. IT-Administratoren müssen nicht nur bestimmte Programme blockieren oder zulassen, sondern auch das Verhalten dieser Programme steuern können, beispielsweise, welche Ressourcen sie nutzen können, auf welche Benutzerdaten die Programme zugreifen und welche sie ändern können, ob Einträge in der Registrierung erlaubt sind usw. Anhand dieser Informationen können Sie Programme davon abhalten, Aktivitäten auszuführen, die eine Gefahr für den Endpoint und das mit ihm verbundene Netzwerk bedeuteten könnten.

  Eine kontinuierliche Echtzeitüberprüfung des Zugriffs auf Programme (Zugriffsart und Person) ermöglicht Ihnen das Erstellen von Verwendungsmustern. Anhand dieser Muster lassen sich die Richtlinien unter Berücksichtigung von Endbenutzeranforderungen und Bedrohungen optimieren.

Whitelists: Leistungsfähigkeit und Kontrolle als Kern des Verfahrens

Programmkontrolle kann als Methode für einen effektiven Schutz vor komplexen Bedrohungen angesehen werden. Dynamische Whitelists sind die treibende Kraft für diesen Vorgang. Die Whitelist-Technologie ist eines der bewährten Verfahren bei jeder erfolgreichen Strategie zur Programmkontrolle. Einfach ausgedrückt: Wenn Sie nicht über Whitelists verfügen, liegt keine echte Programmkontrolle vor.

Whitelists sind Listen vertrauenswürdiger Programme, mit denen IT-Experten ihren bestehenden Kontrollverfahren eine weitere Sicherheitsebene hinzufügen können. Bei jedem Ausführungsversuch eines Programms wird automatisch eine Überprüfung anhand der Whitelist vorgenommen. Ist das Programm in der Liste enthalten, kann es unter den vom Administrator festgelegten Regeln und Richtlinien ausgeführt werden. Wenn das Programm nicht in der Whitelist aufgeführt ist, wird es so lange blockiert, bis der Administrator es genehmigt. Stellen Sie sich dies wie einen „Türsteher“ für Ihren Endpoint vor.



Ziehen Sie einen Default-Deny-Ansatz beim Whitelisting in Betracht

Angesichts der sich ständig ändernden Angriffsmöglichkeiten wird der Default-Deny-Ansatz zunehmend als äußerst wirksame Sicherheitsmethode betrachtet. Dabei wird die Ausführung aller Programme auf allen Workstations blockiert, und es werden nur die explizit vom Administrator zugelassenen Programme ausgeführt.

Das hört sich zwar genau nach der Art von „Alles Blockieren“-Strategie an, die im Büro sehr unbeliebt sein kann, aber wenn eine Default-Deny-Strategie auf effektivem Whitelisting beruht, ist für den Benutzer dennoch eine gewisse Flexibilität gegeben.

Es geht nicht so sehr darum, absolut alles zu blockieren, sondern präzise festzulegen, welche Programme zugelassen werden.

Am besten finden Sie heraus, wie sich ein Default-Deny-Szenario auf Ihr Unternehmen auswirkt, indem Sie es ausprobieren. In einer Sandbox-Umgebung können Sie die tatsächlichen Auswirkungen bei einer Implementierung von Default Deny auf Ihrem IT-System beobachten und verschiedene Anpassungen testen, ohne dass sich dies störend auf das System oder die Benutzer auswirkt. Wahrscheinlich werden Sie überrascht sein, wie wenig sich diese Strategie in der Praxis auf Ihre Benutzer auswirkt.

Einsatz von Whitelisting-Datenbanken

Sie haben sich also für die Arbeit mit Whitelisting entschieden, können aber nicht Ihre gesamte Arbeitszeit darauf verwenden, Listen akzeptabler und „sicherer" Programme zusammenzustellen, zu überprüfen und zu aktualisieren. Bedenken Sie, dass es sich nicht nur um einige wenige Unternehmensprogramme handelt, sondern auch um Geräte wie Drucker, Software für die Netzwerkinfrastruktur sowie Updates.

Dynamische, fortlaufend aktualisierte und überprüfte Whitelist-Datenbanken sind das Herzstück der meisten Lösungen zur Programmkontrolle. So können Administratoren sich mit anderen Aufgaben befassen, während die automatisierten Whitelists effektiv im Hintergrund arbeiten.

Weitere, möglicherweise erforderliche Tools

Eine hochwertige Lösung zu Whitelists und Programmkontrolle ermöglicht Ihnen die Implementierung anhand bewährter Verfahren, ohne komplexe manuelle Auswahl aus den Tausenden von Softwarekomponenten, auf die sich selbst kleine Unternehmen bei ihren täglichen Aufgaben stützen. Ihre Arbeit wird durch eine solche Lösung nicht nur erleichtert, sie umfasst dazu unter anderem folgende wichtige Best-Practice-Verfahren:

- **Bestandsaufnahme**: Sie können nur messen, was Sie auch erfasst haben. Daher wird bei den besten Whitelisting-Programmen zunächst eine Software-Bestandsaufnahme durchgeführt. Hierbei stellen Sie Informationen zu allen im Netzwerk installierten Softwareprogrammen in einem übersichtlichen Format zusammen, das eine einfache Analyse zulässt. Wählen Sie zur Einfachheit eine Lösung mit einer automatischen Bestandsaufnahme aus. Dies erspart Ihnen Zeit (und Mühe) für das Auffinden jeder einzelnen Softwarekomponente im gesamten Unternehmen. Ein weiterer Vorteil besteht darin, dass Sie dabei nicht mehr benötigte Programme entfernen können.

- **Kategorisierung**: Ermöglicht das Zuweisen von Funktionskategorien zu installierter Software (z. B. Betriebssysteme, Unternehmenssoftware, Entwicklungstools, Peripheriegeräte, Browser, Multimedia). So können Administratoren geschäftsrelevante Programme leicht ermitteln und Programme blockieren, die nicht zur Produktivität beitragen. Ein intelligenter Einsatz von Kategorien bedeutet, dass Sie nicht genau herausfinden müssen, mit welchen Spielen die Benutzer ihre Zeit verbringen: Sie können einfach die gesamte Kategorie blockieren. Darüber hinaus können Sie der Liste weitere Programme hinzufügen, die Ihre Benutzer möglicherweise in Zukunft entdecken. Und Ihre Tests mit Default Deny führen möglicherweise dazu, dass Sie weitere Kategorien einrichten.

- **Vertrauenswürdige Updates**: Stellen Sie sicher, dass zugelassene Software regelmäßig aktualisiert wird, um neue oder bisher nicht erkannte Schwachstellen auszumerzen. Dazu gehören Patching, Systems Management-Prozesse und andere Programme für Software-Deployment.

- **Implementierung flexibler Regeln**: Hochwertige Lösungen enthalten eine Vielzahl vordefinierter Regeln für die gängigsten Szenarien. Dies ist eine große Hilfe für den Einstieg in Whitelists. Mit zunehmender Erweiterung Ihrer Whitelist ist aber anzunehmen, dass Sie die Einstellungen auf die speziellen Gegebenheiten Ihres Unternehmens anpassen möchten.

  Beschränken Sie sich nicht mit einer Lösung, die keine flexiblen Anpassungsmöglichkeiten bietet. Sie benötigen Optionen für Aspekte wie Dateinamen, Quellordner oder Anbieter. Weiterhin ist eine flexible Handhabung des MD5- oder „Hashwerts" („Fingerabdruck" für Daten) erforderlich. Dieses Verfahren hindert Kriminelle (und auch Mitarbeiter) daran, die Whitelist durch Tarnen verbotener Programme und Dateien als legitim zu umgehen.

- **Global denken, lokal agieren**

  Sie sollten immer mit einer globalen, umfassenden und dynamischen Whitelist-Datenbank arbeiten. Aber Sie haben nicht die Zeit und Ressourcen, eine solche Liste selbst zusammenzustellen: Die Whitelist-Datenbank von Kaspersky Lab umfasst beispielsweise über 500 Millionen Einzeldateien.

  In der Regel lädt Kaspersky Lab täglich über eine Million Dateien hoch, ein Arbeitsumfang, der ein spezielles Whitelisting-Lab auslasten kann. Diese globalen Datenbanken müssen ständig verfügbar und über die Cloud zugänglich sein. Da die Anbieter vieler führender Unternehmensprogramme ihre Produkte ständig aktualisieren bzw. neue Versionen einführen, lässt sich das Risiko von Fehlalarmen durch fortlaufend aktualisierte globale Datenbanken verringern.

  Datenbanken auf globaler Ebene sind zwar erforderlich, das bedeutet aber nicht, dass Sie keine eigene, rein lokale Whitelist-Datenbank für Ihr spezielles Netzwerk aufstellen sollten. Wählen Sie eine Lösung, die dies unterstützt, besonders, wenn Sie auch eigene Programme entwickeln.

- **Der Clou: das „Golden Image"**

  Ein „Golden Image" ist Ihre Vorlage für die perfekte Installation: Alle unternehmenswichtigen Programme und Einstellungen werden anhand von Best Practices implementiert und genau im Hinblick auf eine optimale Leistung abgestimmt.

  In der Praxis haben IT-Fachleute nur selten die Chance, etwas von Grund auf neu zu schaffen. Sie sollten aber auf jeden Fall ein Golden Image entwickeln, ganz gleich, ob Sie mit brandneuen Computern arbeiten, die noch nie mit dem Internet verbunden waren, oder Ihre Whitelist für bereits vorhandene Technologien nach und nach anpassen. Sehen Sie das Golden Image entweder als Leitfaden für den Aufbau Ihrer Programmkontrolle an, oder nutzen Sie es als Plattform für die Default-Deny-Strategie. Mit einer Lösung, die das Erstellen und Entwickeln eines solchen Golden Image ermöglicht, gestaltet sich der Vorgang für Sie jedenfalls erheblich einfacher, besonders, wenn dazu eine vordefinierte „globale" Vorlage bereitgestellt wird.

Blacklist oder Whitelist? Beides!

Da Whitelists nur die Ausführung vorab genehmigter Programme zulassen, sind sie das Gegenteil herkömmlicher Antiviren-Produkte (auch „Blacklists" genannt), mit denen als schädlich definierte Software blockiert wird. Durch Kombination der beiden Technologien schließen Sie nicht nur die Vordertür, sondern auch die Hintertür Ihres IT-Gebäudes sicher ab.

Die Verknüpfung von Whitelists und Blacklists bietet ein mehrschichtiges Schutzszenario mit bewährten Verfahren und somit maximale Sicherheit. Whitelists können sich sogar positiv auf die Antiviren-Prozesse auswirken, da für Programme auf der Whitelist nicht dieselben intensiven und regelmäßigen Überprüfungen erforderlich sind, wie für Blacklists. Dadurch werden die Systemressourcen geschont und die Programmleistung gesteigert.

3. RICHTIGE VERWENDUNG DER GERÄTEKONTROLLE

Sie haben jetzt die Kontrolle darüber, welche Programme auf Ihren Endpoints ausgeführt werden können und welche nicht. Als Nächstes müssen Sie die gleiche Art von Kontrolle für Ihre Geräte einrichten.

Durch die zentrale Verwaltung von Richtlinien zur Verwendung von Wechseldatenträgern und Medien – USB, Flash-Laufwerke, CD/DVD, Smart Cards usw. – können Sie die von Insidern ausgehenden Risiken erheblich reduzieren. Vielleicht machen Sie sich Gedanken darüber, ob ein unzufriedener Mitarbeiter möglicherweise vertrauliche Daten auf einen USB-Stick kopiert, oder Sie möchten ganz einfach verhindern, dass infizierte tragbare Geräte mit Ihrem Endpoint oder Netzwerk verbunden werden. Eine effektive Gerätekontrolle ist die flexible Lösung für Ihre Probleme.

Hier sind einige nützliche Ansätze für die Einführung eines Programms zur Gerätekontrolle:

- **Definition von Klassen**: Unterschiedliche Geräte haben unterschiedliche Funktionen und stellen somit verschiedenartige Bedrohungen dar. Es wäre eine relativ einfache Entscheidung, beispielsweise einen Default-Deny-Ansatz mit einem Image-Scanner zu verfolgen. Wenn Sie aber z. B. einen USB-Port deaktivieren, hindern Sie diesen Port gleichzeitig daran, einen sicheren, Token-basierten VPN-Zugriff zu unterstützen. Daher brauchen Sie ...
- **Fein abgestufte Einstellungen**: Sie müssen in der Lage sein, unterschiedliche Regeln für verschiedene Geräte sowie Benutzer und Anwendungsszenarien aufzustellen. Administratoren müssen Richtlinien wie Schreibschutz, Blockieren, Lese- und Schreibberechtigung auf unterschiedliche Geräte anwenden können.

  Im Rahmen dieser detaillierten Einstellungen sollte der Administrator auch festlegen können, welche Art von Dateien übertragen werden dürfen, um welche Tageszeit eine bestimmte Richtlinie aktiv wird und welche Geräte wann zugelassen sind. Ihre Arbeit wird sich erheblich einfacher gestalten, wenn Sie diese Regeln gleichzeitig auf mehrere Geräte anwenden können.

  Im Hinblick auf eine noch größere Kontrolle muss es möglich sein, die Richtlinie auf eine bestimmte Seriennummer eines Geräts anzuwenden. Anschließend können Sie Richtlinien und Berechtigungen für bestimmte Gerätemodelle und individuelle Benutzer festlegen und andere Mitarbeiter am Zugriff auf die Daten auf bestimmten Geräten hindern.
- **Zugriffskontrolle**: Dies ermöglicht Ihnen umfassende Kontrolle über den Zugriff ausgewählter Benutzer und Gruppen in einem spezifischen Zeitraum auf bestimmte Gerätetypen. Dies ist u. U. sehr nützlich, wenn Sie beispielsweise die Kosten für das Ausdrucken von Dokumenten außerhalb der Geschäftszeiten senken wollen.

- **Verschlüsselung**: Zu den Best-Practice-Verfahren für das Gerätemanagement gehört immer eine Verschlüsselungskomponente. Es bedarf keiner näheren Erläuterung, wie leicht USB- oder Flash-Laufwerke abhandenkommen oder gestohlen werden können. Die Verschlüsselung kann für bestimmte Gerätetypen anhand von Richtlinien erzwungen werden.
- **Integration mit Active Directory**: Sie können nicht persönlich dafür sorgen, dass jeder einzelne Benutzer im Unternehmen die Richtlinien anwendet. Legen Sie daher einfach die gewünschten Richtlinien für die Gerätekontrolle fest, und setzen Sie sie per Push-Technologie für die Benutzer durch.

4. ARBEITEN SIE ALLEIN?

Eine letzte Frage – wer übernimmt alle diese Aufgaben? Vielleicht Sie selbst? Und ist dies der volle Umfang Ihrer IT-Aktivitäten? Das Arbeiten mit Kontrolltools oder das Sicherheitsmanagement generell macht wahrscheinlich nur einen Teil Ihrer Arbeit aus. Wir hoffen aber, dass Ihr Unternehmen sich genauso bewusst wie wir darüber ist, wie wichtig diese Aufgabe ist.

Ob Sie allein oder als Teil eines kleinen Teams arbeiten, Sie müssen die Sicherheit in Ihrem Unternehmen umfassender und von einem Bildschirm aus kontrollieren können, statt zwischen verschiedenen Konsolen hin- und herzuwechseln.

Andererseits gehören Sie möglicherweise einem großen Sicherheitsteam an, sodass Ihre Verantwortung in einem ganz bestimmten Bereich liegt, z. B. beim Device Management. In diesem Fall benötigen Sie ein Sicherheitssystem mit rollenbasierten Zugriffskontrollen (RBAC), damit Sie allein die Sicherheit in diesem Bereich steuern können.

Es sollte aber keinen Unterschied machen. Es gibt keinen Grund, warum ein einzelner Mitarbeiter nicht die gleichen Sicherheitskontrollen übernehmen kann, wie unterschiedliche Mitglieder eines geschäftigen Teams. Die Frage liegt allein in der Integration. Ein Sicherheitssystem, bei dem alles über eine einzige Plattform gesteuert wird, kann dabei wirklich keine schlechte Sache sein.

ZU GUTER LETZT ...

Angesichts der sich ständig ändernden, vielfältigen Bedrohungen reicht es nicht mehr aus, dass Unternehmen Malware und andere Bedrohungen erkennen und anschließend blockieren. Eine leistungsstarke Blacklisting-Technologie ist auch weiterhin Teil jeder guten Sicherheitsstrategie, aber ein wirklich umfassender Schutz kann nur mit einem mehrschichtigen Ansatz gewährleistet werden.

Sie müssen Ihr Unternehmen einerseits vor herkömmlicher Malware schützen können, andererseits aber auch vor Bedrohungen durch scheinbar legitime Quellen: Schwachstellen in vertrauenswürdigen Programmen, schädlicher Code in beliebten Webseiten, Phishing-Angriffe in E-Mails oder schädliche Software, mit der die automatischen Ausführungsfunktionen bei tragbaren Medien ausgenutzt werden.

Die spezielle globale Whitelisting-Datenbank von Kaspersky Lab ist weltweit führend: Wir sind das einzige Unternehmen für IT-Sicherheit, das ein dediziertes Whitelisting-Labor mit einem eigenen Expertenteam betreibt. Die Software wird über eine einzige, zentrale Konsole gesteuert. Für Sie bedeutet dies maximale Kontrolle mit minimalem Aufwand.


Twitter.com/
Kaspersky_DACH


Facebook.com/
Kaspersky.Lab.DACH


Youtube.com/
KasperskyLabCE

Kaspersky Lab ZAO,
Moskau, Russland
www.kaspersky.de

Informationen zur
Internetsicherheit:
www.viruslist.de

Informationen zu Partnern
in Ihrer Nähe finden Sie hier:
http://www.kaspersky.com/de/partner_finden

KASPERSKY lab