UNTERNEHMENSSICHERHEIT WIRD ANPASSUNGSFÄHIG

Die heutige Bedrohungslage wäre noch vor einem Jahrzehnt praktisch unvorstellbar gewesen. Cyberkriminelle haben ihre Methoden angepasst, um herkömmliche Verteidigungssysteme zu umgehen und legen sich unbemerkt für Monate oder sogar Jahre in Netzwerken auf die Lauer. Für die IT-Sicherheit in Unternehmen wird es Zeit, sich daran anzupassen – durch einen erkenntnisorientierten, mehrstufigen Verteidigungsansatz.

„Intelligenz ist die Fähigkeit, sich an Veränderungen anzupassen."
– Stephen Hawking.

UNTERNEHMENSSICHERHEIT WIRD ANPASSUNGSFÄHIG

APTs (Advanced Persistent Threats), ausgeklügelte Malware und gezielte Angriffe sind nur einige der neuartigen, sich ständig weiterentwickelnden Bedrohungen, denen Unternehmen sich stellen müssen. Cyberkriminelle kennen die Einschränkungen traditioneller, auf Sicherheitsperimetern basierender Verteidigungssysteme nur zu genau – sie sind ihre erste Anlaufstelle bei der Suche nach Lücken in der Verteidigung.

Geht man davon aus, dass die Angreifer ihre Methoden laufend abwandeln, kann man mit Fug und Recht behaupten, dass die Vielzahl der unterschiedlichen in Unternehmen eingesetzten Technologien eine äußerst breite Palette von möglichen Angriffsvektoren bietet: Mobile Geräte, Webanwendungen, Wechseldatenträger, Virtualisierung, Cloud-basierte Technologien bieten Cyberkriminellen allesamt hervorragende Angriffsmöglichkeiten, die mithilfe traditioneller, auf „Verhindern und Abblocken" ausgerichteter Sicherheitsmaßnahmen alleine nicht eliminiert werden können.

Ein neuer, anpassungsfähigerer, integrierter Ansatz, der auf vier zentralen Säulen – Prognose, Prävention, Erkennung und Reaktion – aufbaut, ist erforderlich.

DIE VIER SÄULEN DER ANPASSUNGSFÄHIGEN IT-SICHERHEIT IN UNTERNEHMEN

Prognose: Wir können zwar nicht hellsehen, aber Unternehmen mit Zugriff auf aktuelle Daten zu Bedrohungen und Trends können Sicherheitsvorfälle wesentlich besser antizipieren und vermeiden. Mitarbeiter darin zu schulen, spezifische Angriffstaktiken zu erkennen, ermöglicht eine effektivere prädiktive Analyse, genau wie die Fähigkeit, durch die Analyse von Sicherheitsvorfällen aus Fehlern zu lernen. Penetrationstests hingegen helfen dabei, Schwachstellen aufzudecken.

Prävention: Eine wichtige Aufgabe der Prävention ist es, die Angriffsfläche zu verringern – sei es durch herkömmliche, signaturbasierte Anti-Malware-Verfahren, Gerätekontrollen oder das Schließen von Schwachstellen in Programmsoftware. Systeme zu „härten" und den Angreifern so viele Hindernisse wie möglich in den Weg zu legen, sind nur zwei Bestandteile eines allgemeinen Verteidigungsansatzes, der darauf ausgelegt ist, die Ausbreitung und die Auswirkungen von Angriffen einzudämmen.

Erkennung: Wie wir durch die Erforschung von hochkarätigen APT nachgewiesen haben, können raffiniert aufgebaute Attacken über Jahre hinweg unentdeckt bleiben. Je eher ein Angriff erkannt wird, desto besser. Trotzdem bleiben Angriffe auf Großunternehmen Schätzungen zufolge im Durchschnitt länger als 200 Tage[1] unentdeckt. Erkennungstechnologien, die von einer hochwertigen Bedrohungsanalyse gestützt werden, liefern bessere Ergebnisse: Da sich Bedrohungen rasch entfalten, basiert die effektivste Strategie meist auf der Fähigkeit, Verhaltensweisen und Ereignisabfolgen zu erkennen, die für eine Sicherheitsverletzung typisch sind.

Reaktion: Eine effektive Unternehmenssicherheit muss in der Lage sein, auf einen Sicherheitsvorfall zu reagieren und seine Auswirkungen abzufedern. Dies kann einerseits durch „Wenn/dann"-Regeln zur Ausführung automatisierter Abläufe, z. B. für das Patching, bewerkstelligt werden. Anderseits gehört hierzu eine Analyse des Vorfalls oder der Einsatz eines speziellen Vorfallsreaktionsteams, das Angriffe eindämmt, den Schaden minimiert und die Attacken, Sicherheitsvorfälle usw. analysiert.

Aber um wirklich effektiv zu sein, müssen alle diese Funktionen nahtlos als Teil eines mehrstufigen Systems zusammenarbeiten. Erkenntnisorientiert, auf Bedrohungen fokussiert, integriert, ganzheitlich und strategiegestützt: Dies sind die wichtigsten Charakteristika einer globalen und anpassungsfähigen Sicherheitsarchitektur für Unternehmen. Kaspersky Lab besitzt alle Voraussetzungen, um eine solche anpassungsfähige Sicherheitsplattform für Unternehmen zu entwickeln. Schauen wir uns einmal einige ihrer Elemente an.

[1] https://www.siliconrepublic.com/enterprise/2014/04/11/advanced-cyberattacks-can-go-undetected-for-typically-229-days

UNSER WISSEN. IHR SICHERES UNTERNEHMEN.

Kaspersky Lab kann auf eine lange Erfolgsgeschichte bei der Entdeckung von hochkarätigen, maßgeblichen Cyberbedrohungen zurückblicken. Hierzu gehören u. a.:

- Carbanak: der größte Online-Banküberfall der Welt
- Dark Hotel, das es speziell auf führende Mitarbeiter auf Dienstreise abgesehen hat
- The Mask/Careto mit Fokus u. a. auf Großunternehmen, Behörden und Privatkapitalgesellschaften
- Wild Neutron, das multinationale Konzerne und andere Unternehmen angegriffen hat
- Icefog, das die Lieferkette von Unternehmen angegriffen hat
- Red October: nutzte Unternehmenssysteme für groß angelegte Überwachungsoperationen

Mehr als ein Drittel unserer Mitarbeiter ist im Bereich Forschung und Entwicklung tätig und konzentriert sich ausschließlich auf die Entwicklung von Technologien für Abwehr und Antizipation der sich ständig weiterentwickelnden Bedrohungen, die täglich von unseren Forschungs- und Analyseteams hier bei Kaspersky Lab untersucht werden.

Unser genaues Verständnis der Funktionsweise vieler der weltweit raffiniertesten Bedrohungen hat uns in die Lage versetzt, ein mehrstufiges, strategisch ausgerichtetes Portfolio aus Sicherheitstechnologien und -services zu entwickeln, das ein vollständig integriertes, anpassungsfähiges Sicherheitsmodell möglich macht. Unsere Expertise ist der Grund dafür, dass Kaspersky Lab mehr erste Plätze bei unabhängigen Tests zur Erkennung und Abwehr von Bedrohungen erzielt hat als die meisten anderen IT-Sicherheitsunternehmen.

PROGNOSE

Prognosefähigkeiten – und die Strategien zur Risikominimierung, die mit ihnen Hand in Hand gehen – spielen bei Kaspersky Lab eine zentrale Rolle, angefangen bei unserem internationalen Forschungs- und Analyseteam (GReAT), über das Kaspersky Security Network (KSN), bis hin zu unserem Portfolio aus verschiedenen Security Intelligence Services (SIS):

Kaspersky Security Network: Das Kaspersky Security Network ist eine der wichtigsten Komponenten der mehrstufigen Sicherheitsplattform von Kaspersky Lab. Diese Cloud-basierte, komplexe und verteilte Architektur dient der Erfassung und Analyse von Informationen zu Sicherheitsbedrohungen aus Millionen von Systemen auf der ganzen Welt.

KSN ist im Grunde ein globales, Cloud-basiertes Labor zur Erforschung von Cyberbedrohungen, das in der Lage ist, unbekannte und hochentwickelte Bedrohungen und die Quellen von Online-Attacken innerhalb von Sekunden aufzudecken und zu analysieren – und die gewonnenen Erkenntnisse direkt in die Systeme unserer Kunden einspeist. Für Unternehmen mit speziellen Anforderungen an die Vertraulichkeit ihrer Daten hat Kaspersky Lab das Kaspersky Private Security Network entwickelt.

Security Intelligence Services: Nur wenige Unternehmen haben die Ressourcen, um den Grad an strategischer Sicherheitsexpertise zu entwickeln, der erforderlich ist, um mit den sich ständig weiterentwickelnden, raffinierten Bedrohungen Schritt zu halten. Aus diesem Grund hat Kaspersky Lab ein umfangreiches Portfolio aus Intelligence Services entwickelt:

Ausbildung und Schulung: Von den Grundlagen der Cybersicherheit bis hin zu Schulungen in den Bereichen erweiterte digitale Forensik, Malware-Analyse und Reverse Engineering hält Kaspersky Lab ein umfangreiches Angebot aus Schulungen und Sensibilisierungsprogrammen bereit, die sowohl am Standort als auch online ausgeführt werden. Zusätzlich zu interaktiven Spielen, Assessments zu erlernten Fertigkeiten und der Förderung der allgemeinen Cybersicherheit bieten wir zwei- bis fünftägige Kurse, u. a. zu den folgenden Themen, an:

- **Grundlagen der Cybersicherheit:** Verständnis der Bedrohung, sichere Nutzung von Technologien.
- **Allgemeine digitale Forensik:** Aufbau eines digitalen Forensiklabors, Vorfallsrekonstruktion, Tools.
- **Allgemeine Malware-Analyse und Reverse Engineering:** Aufbau einer sicheren Umgebung für die Malware-Analyse, Ausführen von Schnellanalysen.
- **Erweiterte digitale Forensik:** Tiefgreifende Analyse des Dateisystems, Wiederherstellung gelöschter Dateien, Rekonstruktion des zeitlichen Ablaufs von Vorfällen.
- **Fortgeschrittene Malware-Analyse und Reverse Engineering:** Analyse des Exploit-Shellcodes, Malware für Nicht-Windows-Systeme, Nutzung allgemeiner Best Practices.

Sicherheits-Assessment:

- **Penetrationstests:** Beurteilung der Infrastruktursicherheit aus Perspektive des Angreifers plus gleichzeitige Einhaltung von Sicherheitsstandards wie z. B. PCI DSS.
- **Testen der Programmsicherheit:** Analyse von Webanwendungen (z. B. für Online-Banking und Programme, bei denen WAF aktiviert ist), mobile Programme, Fat-Clients

Informationen zur Bedrohungslandschaft:

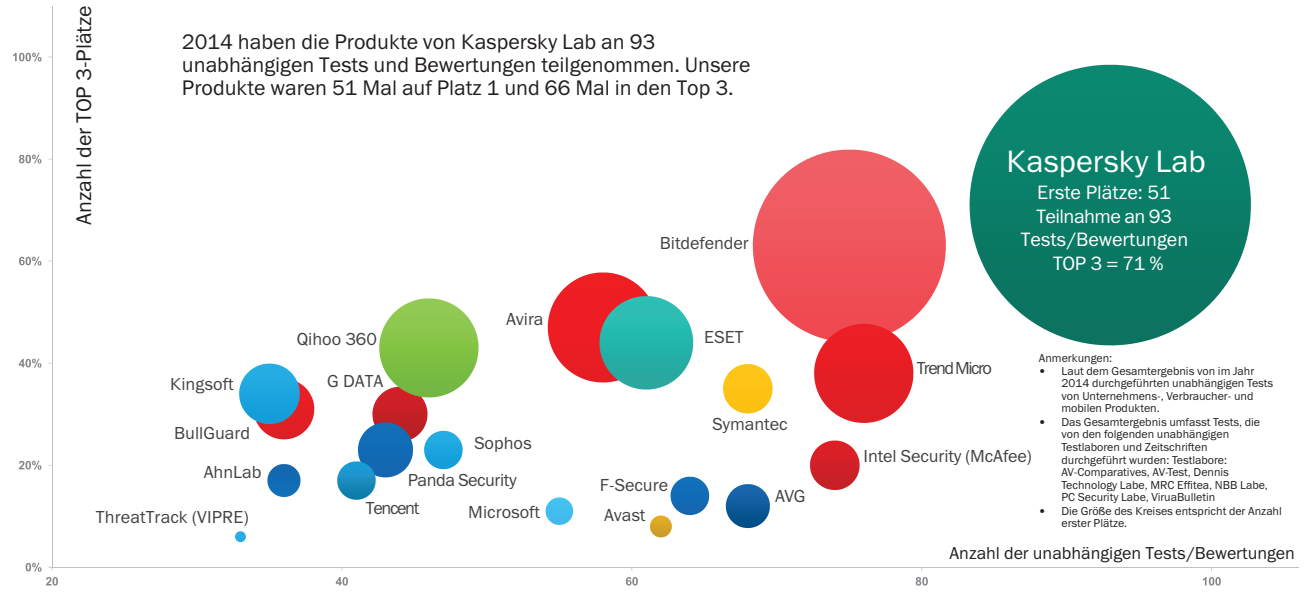
- Dieses auf der Expertise unseres GReAT-Teams und dem Kaspersky Security Network basierende Frühwarnsystem bietet Feeds zur Bedrohungslage, Botnet-Tracking und Berichte über die neuesten Erkenntnisse. Die frühzeitige Verfügbarkeit von APT-Konfigurationsdateien und Malware-Proben sowie die Integration mit SIEM-Lösungen (HP Arcsight) unterstützen Unternehmen bei der Gewinnung umfassender informationsbasierter Erkenntnisse.

PRÄVENTION

Kaspersky Lab entdeckt *jeden Tag* 325.000 neue Malware-Objekte. Selbst ein einziger zusätzlicher Prozentpunkt bei der Erkennungsrate kann zu Hunderttausenden von zusätzlichen Malware-Objekten führen, die nicht durch das Sicherheitsnetz schlüpfen. Unabhängige Testergebnisse belegen übereinstimmend, dass Kaspersky Lab im Branchenvergleich zu den führenden Anbietern zählt. Allein 2014 haben wir an 93 unabhängigen Tests und Bewertungen teilgenommen, aus denen wir 51 Mal als Sieger hervorgingen und in 71 % der Fälle eine Top-3-Platzierung erreichten.[2] Dies ist nur einer der Gründe, warum viele OEMs – darunter Microsoft, Cisco Meraki, Juniper Networks und Alcatel Lucent – Kaspersky Lab die internen Sicherheitsfunktionen ihrer eigenen Produkte anvertrauen.

[2] Weitere Details zu den Tests und Metriken finden Sie unter: http://media.kaspersky.com/en/business-security/TOP3_2013.pdf
Den aktualisierten Bericht finden Sie unter: http://media.kaspersky.com/en/business-security/TOP3_2014.pdf.

KASPERSKY LAB BIETET DEN BESTMÖGLICHEN SCHUTZ*



Unser Lösungsportfolio für Unternehmenssicherheit vereint branchenweit den bestmöglichen Malware-Schutz mit einer Vielzahl unterschiedlicher Technologien zur Verringerung der Angriffsfläche zu einer einzigartigen Kombination von informationsbasierten Technologien.

Bekannte, unbekannte und hochentwickelte Bedrohungen werden durch Schutzmechanismen auf mehreren Ebenen neutralisiert. Hierzu gehören u. a.:

Network Attack Blocker: Untersucht den gesamten Netzwerkverkehr anhand von bekannten Signaturen, um netzwerkbasierte Angriffe, z. B. Port-Scanning und DDoS-Angriffe, zu erkennen und abzuwehren. Kaspersky DDoS Protection (KDP) bietet als separat erhältlich Lösung zusätzlich Schutz vor DDoS-Angriffen (Distributed Denial of Service). Diese umfassende, integrierte Lösung zur Vermeidung und Abwehr von DDoS-Angriffen bietet Funktionen zur kontinuierlichen Analyse und Berichterstellung nach erfolgten Angriffen.

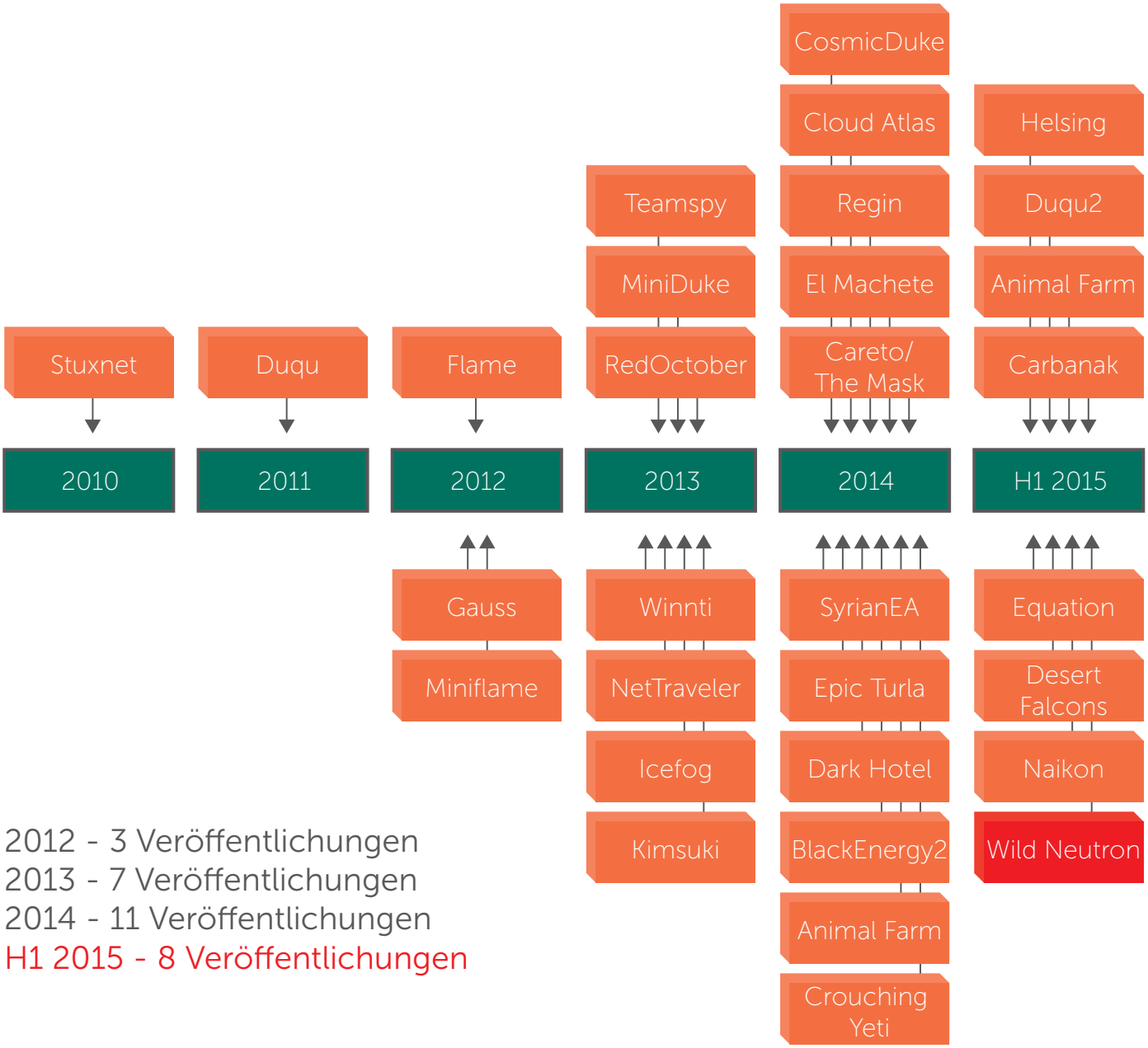
Heuristische Verfahren zur Phishing-Abwehr: Abwehr der allerneusten Phishing-Technologien durch Analyse auf zusätzliche Hinweise auf verdächtige Aktivitäten zusätzlich zu herkömmlichen, datenbankbasierten Phishing-Verfahren.
Programmkontrolle und dynamische Whitelists: Die Programmkontrolle lässt die Ausführungen von Programmen zu, die vom Administrator festgelegt werden, oder blockiert diese. Der Ansatz basiert auf dem dynamischen Whitelisting, eine fortlaufend aktualisierte Liste vertrauenswürdiger Programme und Softwarekategorien.

Host Intrusion Prevention System (HIPS): Kontrolliert das Programmverhalten und schränkt die Ausführung potentiell gefährlicher Programme ein, ohne dadurch die Leistungsfähigkeit von genehmigten, unbedenklichen Programmen zu beeinträchtigen.

ERKENNUNG

Die einzigartige Expertise von Kaspersky Lab bei der Erkennung von hochentwickelten Bedrohungen fließt direkt in die Funktionen zur Erkennung von Bedrohungen für Unternehmen ein. Seit 2008 haben unsere Experten einige der raffiniertesten, aus mehreren Komponenten bestehenden Angriffe entdeckt, die weltweit bisher aufgedeckt wurden. Die dabei gewonnenen Erkenntnisse fließen direkt in unsere Produktentwicklung ein. Neben unserer Fähigkeit, hochentwickelte, speziell gegen Unternehmen gerichtete Attacken zu erkennen, haben wir die Erkenntnisse, die wir bei der Identifizierung von Bedrohungsakteuren, die sich auf den Finanzsektor konzentrieren, wie z. B. Carbanak, zur Entwicklung von Lösungen zur Erkennung von Finanztransaktionsbetrug genutzt.

APT-VERÖFFENTLICHUNGEN DURCH KASPERSKY LAB



2012 - 3 Veröffentlichungen
2013 - 7 Veröffentlichungen
2014 - 11 Veröffentlichungen
H1 2015 - 8 Veröffentlichungen

REAKTION

Innerhalb einer anpassungsfähigen Sicherheitsarchitektur kommt der Reaktion auf Bedrohungen die gleiche Bedeutung zu wie der Fähigkeit, sie vorherzusagen und zu verhindern – sie spart dem Unternehmen Zeit und Geld. Hinzu kommt, dass eine effektivere Erkennung eine verbesserte Reaktionsfähigkeit zur Folge hat. Kaspersky Lab nutzt dies sowohl auf der Technologie- als auch der Service-Ebene:

Aktivitätsmonitor: Unser einzigartiges und proaktives Überwachungssystem reagiert auf komplexe Systemvorgänge, z. B. die Installation von Treibern, und erkennt verdächtige Verhaltensmuster.

Untersuchungsservices: Behebt Sicherheitsvorfälle dank Unterstützung durch Kaspersky Lab in Echtzeit. Durch Malware-Analyse über digitale Forensik bis hin zu Reporting und Vorfallsreaktion erhalten unsere Kunden die Möglichkeit, aus Sicherheitsvorfällen zu lernen, während gleichzeitig die Auswirkungen minimiert und beschädigte Systeme wiederhergestellt werden.

PROAKTIVE, REAKTIVE, ERKENNTNISORIENTIERTE IT-SICHERHEIT FÜR UNTERNEHMEN

Die Behauptung, Malware habe sich wie ein Krebsgeschwür ausgebreitet, ist eine Untertreibung: Hochentwickelte Bedrohungen umgehen herkömmliche Abwehrtechniken, gebrauchsfertige Malware-Kits, die schon für wenig Geld im Internet erstanden werden können, sowie Tools, die automatisch eine Vielzahl von maßgeschneiderten Varianten einer bestimmten Malware generieren können, sind nämlich nur die Spitze einer massiven Malware-Bedrohung.

Eine immer raffinierter und komplexer werdende Bedrohungslage erfordert einen mehrstufigen, anpassungsfähigen Sicherheitsansatz, bei dem eine Kombination aus integrierten Technologien eine umfassende Erkennung und Schutz vor bekannter, unbekannter und hochentwickelter Malware sowie anderen, speziell auf Unternehmen ausgerichteten Bedrohungen bietet.

Dank seiner einzigartigen Erfolgsgeschichte bei der Aufdeckung der raffiniertesten Cyberbedrohungen und branchenweit führender Technologien und Services besitzt Kaspersky Lab alle Voraussetzungen, um Unternehmen die umfassende und anpassungsfähige Sicherheit zu liefern, die sie benötigen. Während das Kaspersky Security Network auf den Echtzeitinformationen von über 60 Millionen Nodes weltweit aufbaut, trägt unser „Global Research and Analysis Team" (GReAT) spezielle Fähigkeiten und Know-how zur Bedrohungsforschung bei und entwickelt Lösungen, die Schutz vor Bedrohungen bieten, der immer komplexer und raffinierter werden.

VERLÄSSLICHER PARTNER VON UNTERNEHMEN, REGIERUNGEN UND BEHÖRDEN

Als privates Unternehmen sind wir in der Lage, hohe Investitionen in unsere Forschung und Entwicklung zu tätigen. Nahezu die Hälfte unserer weltweit 3.000 Mitarbeiter ist in unseren Forschungs- und Entwicklungseinrichtungen tätig und beschäftigt sich primär mit der Entwicklung innovativer Technologien und der Analyse von Cyber-Kriegsführung und -Spionage sowie allen Arten von Bedrohungen und Techniken.

Diese Fokussierung auf eine hochwertige, interne Forschung und Entwicklung hat Kaspersky Lab zu einem der Branchenführer im Bereich IT-Sicherheitstechnologien gemacht. Dies ist nur einer der Gründe, warum über 100 führende OEMs – allen voran Microsoft, Cisco Meraki, Juniper Networks und Alcatel Lucent – Kaspersky Lab die internen Sicherheitsfunktionen ihrer eigenen Produkte anvertrauen.

Und warum wir ein verlässlicher Partner für Regierungen, Strafverfolgungsbehörden und Großunternehmen auf der ganzen Welt sind. Angesehene internationale Unternehmen, darunter INTERPOL, Europol und eine Reihe von CERTS, haben Kaspersky Lab um eine langfristige Zusammenarbeit gebeten. Zusätzlich zu regelmäßigen Schulungen für Beamte von INTERPOL und Europol sowie für Polizeikräfte vieler Länder haben wir auch den Aufbau des digitalen Forensiklabors von INTERPOL unterstützend begleitet.


Twitter.com/
Kaspersky_DACH


Facebook.com/
Kaspersky.Lab.DACH


Youtube.com/
KasperskyLabCE

Kaspersky Labs GmbH
Ingolstadt
Deutschland
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