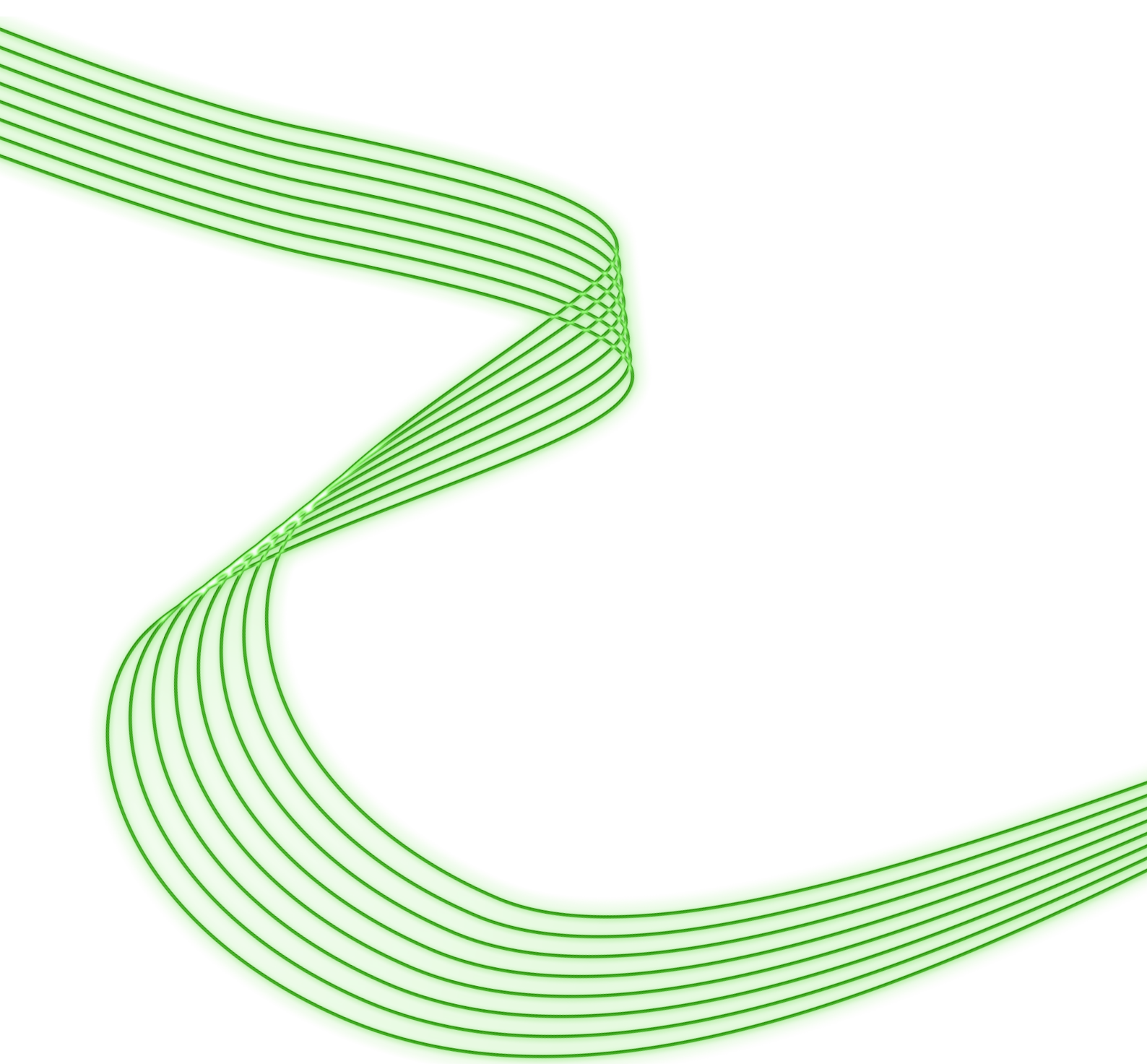


WARUM KOMPLEXITÄT IM WIDERSPRUCH ZU IT-SICHERHEIT STEHT

In diesem Whitepaper wird untersucht, inwiefern Komplexität neue Probleme im Hinblick auf die Sicherheit aufwirft und wie sich diese lösen lassen.

With Kaspersky, now you can.
kaspersky.de/business-security

Be Ready for What's Next

KASPERSKY lab

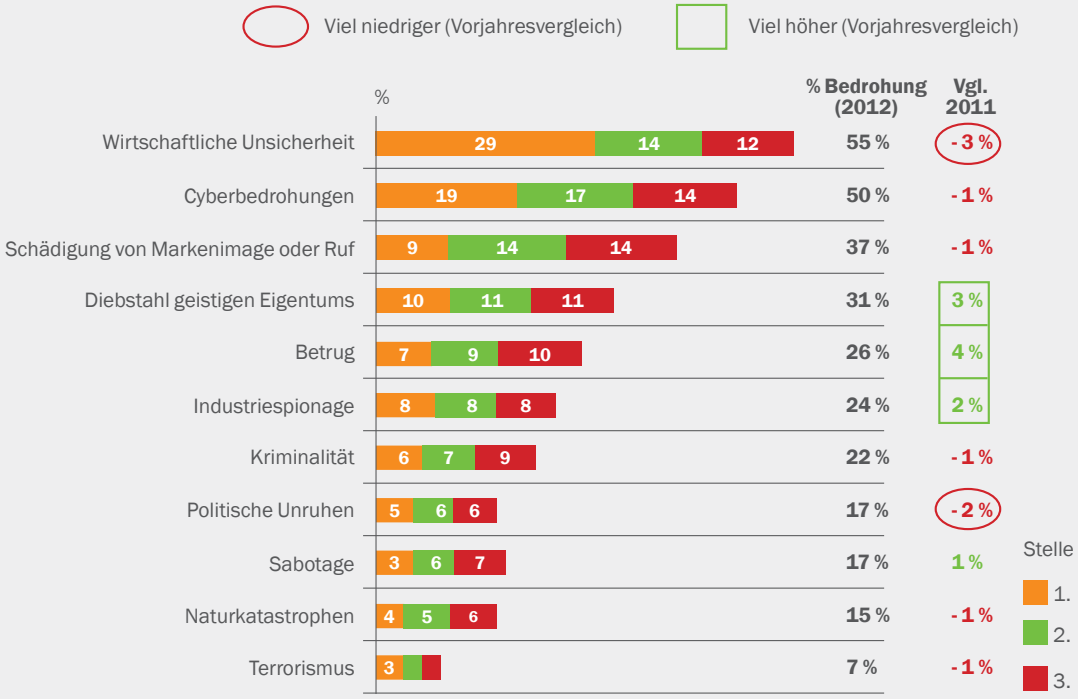
Zusammenfassung

1.0

Unternehmen auf der ganzen Welt streben nach mehr Flexibilität, Effizienz und Innovationen. Gleichzeitig müssen aber auch Kosten gesenkt, die Produktivität gesteigert und die Wettbewerbsfähigkeit verbessert werden. Dabei ist es nach wie vor die IT-Abteilung, die für die Erfüllung dieser Erwartungen zuständig ist.

Für IT ergeben sich daraus neue komplexe Fragestellungen und zusätzliche Aufgaben. Angesichts der zunehmenden Komplexität werden Schwachstellen im System, wie ungepatchte Programme oder neue Geräte im Netzwerk, leicht übersehen. Dies birgt mitunter erhebliche Sicherheitsrisiken. Unternehmen wissen um diese Problematik. Als Kaspersky Lab im Rahmen der **weltweiten Umfrage zu IT-Risiken 2012** über 3.300 IT-Experten aus 22 Ländern zu ihrer Meinung und ihren Erfahrungen befragte, überraschte es nicht, dass Cyberbedrohungen als zweitgrößtes Risiko hinter der wirtschaftlichen Unsicherheit rangierten (Abb. 1).

Abb. 1: Derzeit größte Unternehmensrisiken[1]



Die wichtigsten Technologiebereiche, in denen zusätzliche Ressourcen und Verwaltungstools erforderlich sind, sind mobile Geräte, Verschlüsselung, Steuerungsfunktionen (wie Programm-, Web- und Gerätekontrolle) sowie das Systems Management. Zu den in der von Kaspersky Lab durchgeführten weltweiten Umfrage zu IT-Risiken 2012 (Abb. 2) meistgenannten Problemen zählte zudem die oftmals manuelle Aktualisierung von Patches.

1 Quelle: Weltweite Umfrage zu IT-Risiken 2012 von Kaspersky Lab

„Bei einer optimalen IT-Sicherheit besteht immer ein Gleichgewicht zwischen Risiken, Kosten und Praktikabilität. Das bedeutet aber, dass zur genauen Einschätzung der letzten beiden Punkte der erste vollkommen klar sein muss. Meine Sorge ist, und dies wurde in der Umfrage ja auch bestätigt, dass derzeit die Risiken schneller zunehmen, als die Unternehmen dies wahrhaben wollen."
Chris Christiansen, VP Security Products & Services bei IDC[3]

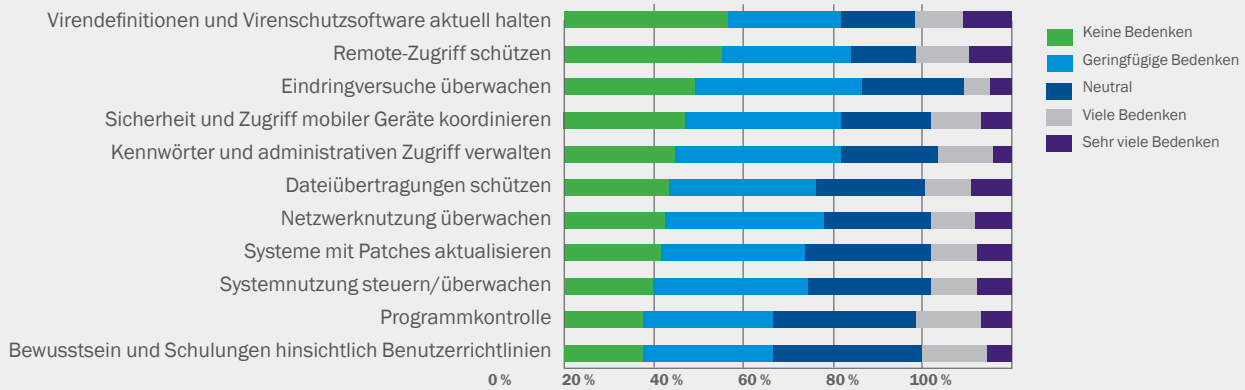
Die derzeitigen IT-Sicherheitslösungen können die mit der Komplexität einhergehenden Probleme noch verschärfen, da es sich in der Regel um gezielte Lösungen für spezielle Probleme handelt, darunter die Verwaltung oder Verschlüsselung mobiler Geräte. Bestenfalls sind diese miteinander verbunden, schlimmstenfalls sind sie nicht miteinander kompatibel. Für IT-Administratoren bedeutet dies, dass sie von einem Dashboard zum nächsten wechseln müssen, um Richtlinien umzusetzen, den Status von Endpunkten zu prüfen und Programme mit Patches zu aktualisieren. Dadurch kann es leicht zu Sicherheitslücken kommen.

Große internationale Unternehmen können in umfangreiche unternehmensweite Technologien und eigenes spezielles Personal investieren, um die Sicherheit ihrer IT zu gewährleisten. Für kleine und mittelständische Firmen aber ist dies nicht möglich. Sie müssen mit weitaus kleineren IT-Abteilungen ähnliche Probleme bewältigen.

Unternehmen sehen sich so Problemen gegenüber, die gleichsam ihre Aufmerksamkeit erfordern: immer mehr geschäftskritische Daten, die Verwaltung einer zunehmend komplexen Umgebung sowie die wachsende Anzahl externer Risikofaktoren.

Diese Tatsache kam insbesondere in der weltweiten Umfrage zu IT-Risiken 2012 von Kaspersky Lab zum Ausdruck[2]. Bei der Auswertung der Umfrageergebnisse sagte Chris Christiansen, VP Security Products & Services bei IDC, „dass *bei einer optimalen IT-Sicherheit immer ein Gleichgewicht zwischen Risiken, Kosten und Praktikabilität besteht. Das bedeutet aber, dass zur genauen Einschätzung der letzten beiden Punkte der erste vollkommen klar sein muss. Meine Sorge ist, und dies wurde in der Umfrage ja auch bestätigt, dass derzeit die Risiken schneller zunehmen, als die Unternehmen dies wahrhaben wollen."*

Abb. 2: Wie sehr machen Sie sich täglich Gedanken über die folgenden IT-Sicherheitsprobleme in Ihrem Unternehmen?[2]



Für Unternehmen, die wissen, welche Anforderungen sie zu erfüllen haben, bedarf es einer neuen Herangehensweise. Diese muss bestehende Standards und Einschränkungen überwinden und IT-Teams, die mit Ressourcenengpässen zu kämpfen haben, die Möglichkeit geben, die IT-Sicherheit auszubauen und gleichzeitig deren Verwaltbarkeit zu gewährleisten.

Dieses Whitepaper stellt die wirklichen Probleme der Unternehmen vor sowie welche neuen Bedrohungen sich daraus für die IT-Sicherheit ergeben. Anti-Malware alleine reicht zunehmend nicht mehr aus. Daher wird in diesem Whitepaper eruiert, welche neue Vorgehensweise im Hinblick auf die IT-Sicherheit erforderlich ist, um auf die neuen Bedrohungen und die veränderten Arbeitsweisen adäquat zu reagieren.

2 Quelle: Weltweite Umfrage zu IT-Risiken 2012 von Kaspersky Lab
3 Quelle: Weltweiter Bericht über IT-Risiken 2012 von Kaspersky Lab

Antriebsfaktoren des Unternehmens: Wodurch entsteht das Problem?

2.0

Die Notwendigkeit einer neuen Herangehensweise im Hinblick auf die IT-Sicherheit ergibt sich aus den Änderungen, die in einem Unternehmen stattfinden und auf die die IT-Abteilung dann reagieren muss. Obwohl diese teilweise die Folge technologischer Anforderungen sind, ergeben sie sich letztendlich doch alle aus der Tatsache, dass Kosten gesenkt, die Flexibilität verbessert und die Produktivität gesteigert werden müssen.

2.1 Technologien
Technologien werden für Unternehmen immer wichtiger. Damit steigt auch die Anzahl der Systeme und Plattformen, die ein effektives Arbeiten erst ermöglichen. Unternehmen aller Größe setzen Technologien immer schneller und in vielfältigen Bereichen ein. Tools zur Zusammenarbeit werden zunehmend verwendet, um die Entscheidungsfindung zu beschleunigen und Reisezeiten und -kosten zu reduzieren. Daneben stellen Unternehmen ihren Mitarbeitern eine Reihe mobiler Geräte zur Verfügung.

All dies führt zu immer größeren Datenmengen sowie der Entstehung neuer Endpunkte, woraus sich wiederum mögliche Einfallstüren für Cyberangriffe ergeben.

2.2 Schlecht vorbereitet und zu wenige Ressourcen?
Die Lösung dieser Schwierigkeiten obliegt dann der IT-Abteilung. Und obwohl deren Aufgaben immer umfangreicher und komplexer werden, bleiben die verfügbaren Mittel und Mitarbeiter oftmals unverändert oder werden gar noch reduziert.

IT-Manager und Administratoren müssen hochgradig flexibel sein. Sie müssen mehrere Aufgaben gleichzeitig erledigen und sich schnell in neue Technologien einarbeiten. So kann es vorkommen, dass am Morgen Server zurückzusetzen und gegen Mittag Firewall-Regeln und Zugriffssteuerungslisten anzupassen sind. Am Nachmittag hingegen geht es um Konfigurationseinstellungen mobiler Geräte, damit das neue Smartphone oder der neue Tablet-Computer des Geschäftsführers auch E-Mails empfangen und auf das Netzwerk zugreifen kann. Und kurz vor Feierabend sind Konflikte bei der Übersetzung von Netzwerkadressen auf Edge-Routern zu beheben. Sicherlich fällt all das in den üblichen Zuständigkeitsbereich von IT-Mitarbeitern. Zu einer Herausforderung werden die Aufgaben aber angesichts der Vielzahl an neuen Technologien und Anforderungen, die es vor wenigen Jahren schlichtweg nicht gab.

2.3 Veränderungen in der Arbeitsweise
Die Mitarbeiter von heute sind daran gewöhnt, anwenderfreundliche und funktionale Technologien selbstverständlich nutzen zu können. Bei ihrer Arbeit setzen sie Tools, Programme und Geräte zur Zusammenarbeit zielstrebig ein.

Zudem erwarten die Mitarbeiter, von überall auf Webdienste zugreifen und jederzeit über erforderliche Programme, Daten und Ressourcen verfügen zu können – und zwar ohne Unterstützung der IT-Abteilung und ohne dass diese ihnen vorgibt, wie oder womit sie zu arbeiten haben. Die Folge hiervon ist eine hohe Erwartungshaltung an die Reaktionsfähigkeit der Unternehmen, quasi eine Nebenwirkung des Technologiekonsums, die es erschwert, Erwartungen so zu erfüllen, wie Unternehmen dies bisher getan haben.

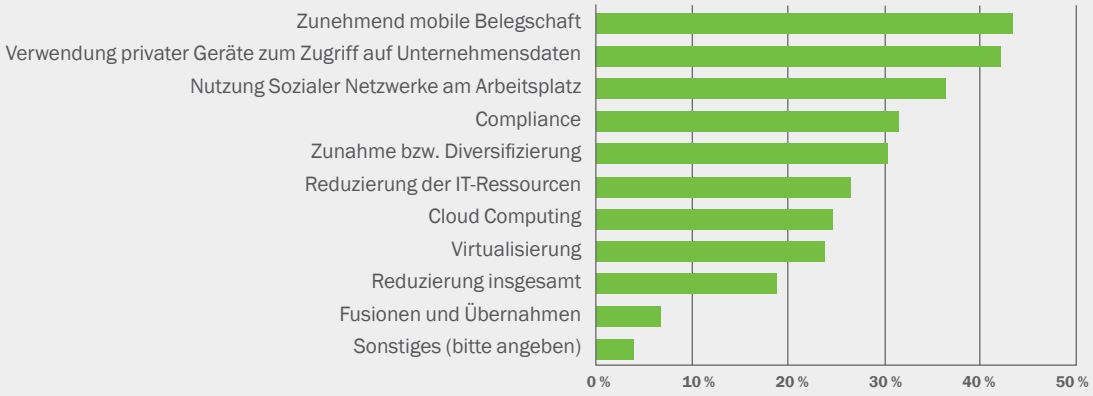
Anstelle die Nutzung eigener Geräte zu verhindern, wird jetzt versucht, mit der neuen Situation zurechtzukommen.

2.4 Mobilität

Im dritten Quartal 2012 berichtete IDC, dass weltweit 444,5 Millionen Smartphones ausgeliefert wurden. Das entspricht einer weltweiten Zunahme von 2,4 % im Vorjahresvergleich.[4] Viele dieser mobilen Geräte werden bei der Arbeit genutzt, und Endanwender betrachten Mobilität als eine Möglichkeit, ihr Geschäfts- und Privatleben zu kombinieren.

Im März 2012 führte Kaspersky Lab zusammen mit dem Forschungsunternehmen Bathwick Group eine internationale Studie mit dem Namen **„Security readiness in a changing technology landscape“ (Abb. 3)** durch. Die Ergebnisse zeigten, dass Mobilität IT-Experten weltweit derzeit die meisten Sorgen bereitet. Die Tatsache, dass immer mehr Mitarbeiter, darunter vorzugsweise leitende Angestellte, ihre Privatgeräte bei der Arbeit einsetzen und dabei auf das Firmennetzwerk zugreifen und Firmendaten nutzen, stellt für die IT ein wachsendes Kontrollproblem dar.

Abb. 3: Welche Probleme bereiten Ihrem Unternehmen die größten Sorgen im Hinblick auf die Sicherheit?[5]



Anstatt die Nutzung eigener Geräte zu verhindern, wird jetzt versucht, mit der neuen Situation zurechtzukommen. In Anbetracht der vielen Gerätetypen, Betriebssysteme, mobilen Programme und weil Mitarbeiter ihre kabellosen oder kabelgebundenen Geräte einfach anschließen und auf Daten zugreifen, ist dies keine einfache Aufgabe. Je größer die Komplexität, desto mehr muss verwaltet werden.

Aufgrund der veränderten Aufgabenstellung für die IT und der sich ändernden Arbeitsweisen und Geschäftsanforderungen wird es spürbar schwieriger, das Gleichgewicht zwischen Ressourcen, Kosten und Sicherheit aufrechtzuerhalten.

4 Laut IDC vom 9. Juni 2011 wird der weltweite Smartphone-Markt 2011 erwartungsgemäß um 55 % wachsen. Die Anzahl der ausgelieferten Geräte wird bis 2015 auf nahezu eine Milliarde ansteigen. http://www.idc.com/getdoc.jsp?containerId=prUS22871611

5 Quelle: Bathwick Group, Security readiness in a changing technology landscape, März 2012

Bedrohungen: so ausgeklügelt wie noch nie

3.0

- Über 67 Millionen einzelne Bedrohungen in der Datenbank von Kaspersky Lab erfasst[6]
- Anzahl der Bedrohungen steigt pro Tag um 125.000[6]
- Täglich 140 neue Malware-Bedrohungen für mobile Geräte[6]
- 91 % der Unternehmen waren in den letzten 12 Monaten mindestens einer Bedrohung ausgesetzt[7]

Die Entwicklung der Cyberrisiken in den letzten Jahren lässt sich mit zwei Schlagwörtern beschreiben: Umfang und Raffinesse. Unterstützt wird dies durch die weltweite Umfrage zu IT-Risiken 2012 von Kaspersky Lab, bei der sich zeigte, dass auf 91 % der Unternehmen in den vorausgegangenen zwölf Monaten mindestens einmal ein Cyberangriff verübt wurde.

Die bei Malware beobachtete Raffinesse ist inzwischen so ausgeklügelt, dass viele der Befragten meinten, ein herkömmlicher Malware-Schutz wäre nicht mehr ausreichend. Stuxnet und Flame haben es sogar bis in die Schlagzeilen gebracht und zwar nicht aufgrund des angerichteten Schadens, sondern weil beide so lange unbemerkt blieben. Flame gibt es bereits seit Jahren und wurde erst im Mai 2012 offiziell entdeckt.

3.1 Eine neue Art von Bedrohungen

Diese Beispiele zeigen, dass es Cyberkriminellen inzwischen um weitaus mehr geht: Viren sind raffinierter und nutzen Schwachstellen im System gezielt mit der Absicht aus, an wertvolle Daten zu gelangen.

Die Bankkonten von Unternehmen sind besonders gefährdet, da sich hier große Geldsummen befinden und die Kontoinhaber nicht immer ausreichend Sicherheitsmaßnahmen ergreifen. Das erklärt sicherlich die wachsende Anzahl an Trojanern und Malware wie Zeus, die Daten stehlen und Hackern die Möglichkeit geben, auf Unternehmensgelder zuzugreifen.

Dieser Trend ist eine Folge des Auftretens hochentwickelter, hartnäckiger Bedrohungen. Behörden und internationale Unternehmen sind längst nicht mehr die einzigen Ziele ausgefeilter Malware-Angriffe. Kleinunternehmen sind ebenso zur Zielscheibe geworden. Und da Cyberkiminelle diese Bedrohungen immer öfter einsetzen, steigt auch das Risiko von Begleitschäden. Das heißt, dass auch Unternehmen, die nicht das eigentliche Ziel eines Angriffs sind, davon betroffen sein können.

3.2 In der Infrastruktur nach oben

Die Anforderungen an die IT-Sicherheit eines durchschnittlichen Unternehmens haben sich angesichts dieser Raffinesse und kriminellen Energie komplett geändert. Angriffe von heute nutzen Schwachstellen in gängigen Programmen aus. Früher stand Windows selbst im Fokus derer, die auf der Suche nach Sicherheitslücken waren, um schädlichen Code auf einem Computer zu installieren. Dank der regelmäßigen Veröffentlichung von Updates seitens Microsoft in den vergangenen Jahren haben Cyberkriminelle ihre Aufmerksamkeit jetzt auf Programme gerichtet, die nicht mit Windows zusammenhängen. Windows ist inzwischen nicht einmal mehr unter den zehn am meisten angreifbaren Softwarepaketen (Abb. 4 und 5). Leider werden für viele Programme über lange Zeit keine Patches veröffentlicht.

6 Quelle: Kaspersky Lab
7 Quelle: Weltweite Umfrage zu IT-Risiken 2012 von Kaspersky Lab

Laut securelist.com werden in über 80 % der Fälle Java und Adobe Acrobat Reader zur Zielscheibe.[8] Java ist auf unzähligen Computern installiert (laut Aussage von Oracle sind es 1,1 Milliarden), die Updates werden aber nur nach Bedarf und nicht automatisch installiert. Bei Adobe Acrobat Reader bieten nur die neuesten Versionen die Möglichkeit automatischer Updates. Benutzer sind daran gewöhnt, Programme auf Computer und Smartphone herunterzuladen und etliche verwaltete und nicht verwaltete Programme zu erstellen. All diese haben mögliche Sicherheitslücken.

Die zunehmende Diversifizierung von Geräten und Betriebsplattformen, mit denen Unternehmen Daten verarbeiten, erhöht die Anforderungen an die IT-Sicherheit. Es gilt, mehr zu verwalten und mehr Schwachstellen auszubessern.

Zwar konzentrieren sich die Sicherheitslücken auf die Plattformen, aber die zunehmende Anzahl an Betriebssystemen und die vielen zehntausend dafür entwickelten Programme machen es unmöglich, Sicherheitslücken zu dokumentieren und zu schließen. Dieser Trend zeigt sich in der Vielfalt der angreifbaren Programme und Betriebssysteme (Abb. 4 und 5).

Abb. 4: Meistangegriffene Programme

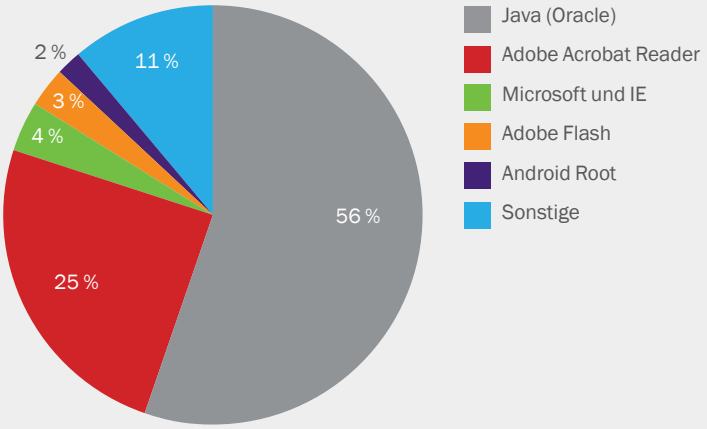


Abb. 5: Oberste zehn Sicherheitslücken in Software, erstes Quartal 2012[9]

Stelle	Angreifbares Programm	% angreifbarer Benutzer	Bewertung
1.	Oracle Java (mehrere Schwachstellen)	35 %	Sehr wichtig
2.	Oracle Java (drei Schwachstellen)	21,7 %	Extrem wichtig
3.	Adobe Flash Player (mehrere Schwachstellen)	19 %	Sehr wichtig
4.	Adobe Flash Player (mehrere Schwachstellen)	18,8 %	Sehr wichtig
5.	Adobe Reader/Acrobat (mehrere Schwachstellen)	14,7 %	Extrem wichtig
6.	Apple Quick Time (mehrere Schwachstellen)	13,8 %	Sehr wichtig
7.	Apple iTunes (mehrere Schwachstellen)	11,7 %	Sehr wichtig
8.	Winamp AVI/IT-Dateiverarbeitung	10,9 %	Sehr wichtig
9.	Adobe Shockwave Player (mehrere Schwachstellen)	10,8 %	Sehr wichtig
10	Adobe Flash Player (mehrere Schwachstellen)	9,7 %	Extrem wichtig

8 Quelle: https://www.securelist.com/en/analysis/204792250/IT_Threat_Evolution_Q3_2012#4
9 Quelle: https://www.securelist.com/en/analysis/204792250/IT_Threat_Evolution_Q3_2012#14

Bedrohungen: so ausgeklügelt wie noch nie

Schwachstellen ausbessern: vermehrte Datenverschlüsselung

- 15 % der Unternehmen erlitten infolge des Diebstahls mobiler Geräte Datenverluste.[11]
- Malware und Spam sind nach wie vor die Hauptursache von Datenverlusten.[11]
- Datenverschlüsselung belegt auf der Liste der Bereiche, die Unternehmen gerne verbessern würden, den zweiten Platz.[11]

3.3 Die Dimension der Mobilität

Mobilität erweitert das Risiko um eine neue Dimension. Heutzutage sind die Betriebssysteme iOS, OS X von Apple und die diversen Betriebssysteme von Google und Android so allgegenwärtig wie Windows.

Wenn es darum geht, die durch Mobilität verursachten Risiken auszunutzen, haben Cyberkriminelle schon einen gewaltigen Vorsprung. Im Vergleich zum ersten Quartal 2012 verdreifachte sich im zweiten Quartal die Zahl der auf Android gerichteten Trojaner nahezu (Abb. 6).

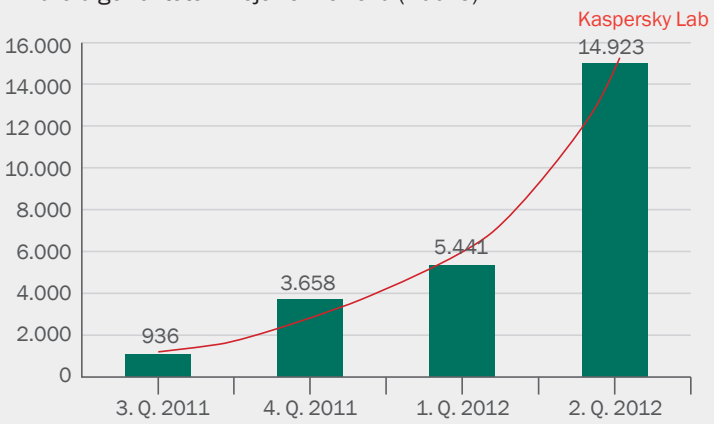


Abb. 6: Anzahl der auf das Android-Betriebssystem ausgerichteten Malware-Modifikationen[10]

Dies wird weiter zunehmen, da die Einfachheit mit der sich mobile Daten von Geschäftstätigen abrufen lassen, dazu führt, dass Cyberkriminelle Mobilität ausnutzen.

In der weltweiten Umfrage zu IT-Risiken 2012 von Kaspersky Lab zeigte sich die Tendenz von Mitarbeitern, mit privaten Geräten zu arbeiten, sowie, dass immer mehr Unternehmen ihren Angestellten ohne zusätzliche Sicherheitsmaßnahmen erlauben, mit diesen Geräten Unternehmensdaten abzurufen und auf das Netzwerk zuzugreifen. Diese überraschend laxe Handhabung ist einer Reihe von Faktoren geschuldet, mehrheitlich aber der wachsenden Geräteanzahl sowie der Tatsache, dass es einfach zu viele Gerätetypen und Versionen von Betriebssystemen gibt, als dass ein mit zu wenigen Ressourcen ausgestattetes IT-Team diese kontrollieren und verwalten könnte.

Aufgrund von Drahtlosverbindungen, Cloud-Diensten und Programmen zur Dateisynchronisierung werden solche Geräte gerne gestohlen.

Mit den gestohlenen Geräten rufen Diebe und Hacker dann wertvolle Daten ab oder greifen auf Firmennetzwerke zu. Der aus Diebstahl und Verlust von Geräten entstehende finanzielle Schaden wird auf jährlich 7 Millionen US-Dollar geschätzt.[12] Die indirekten Kosten damit zusammenhängender Hacking-Vorfälle sind nicht bekannt.

3.4 Soziale Netzwerke: trotz steigendem Risiko weniger Einschränkungen

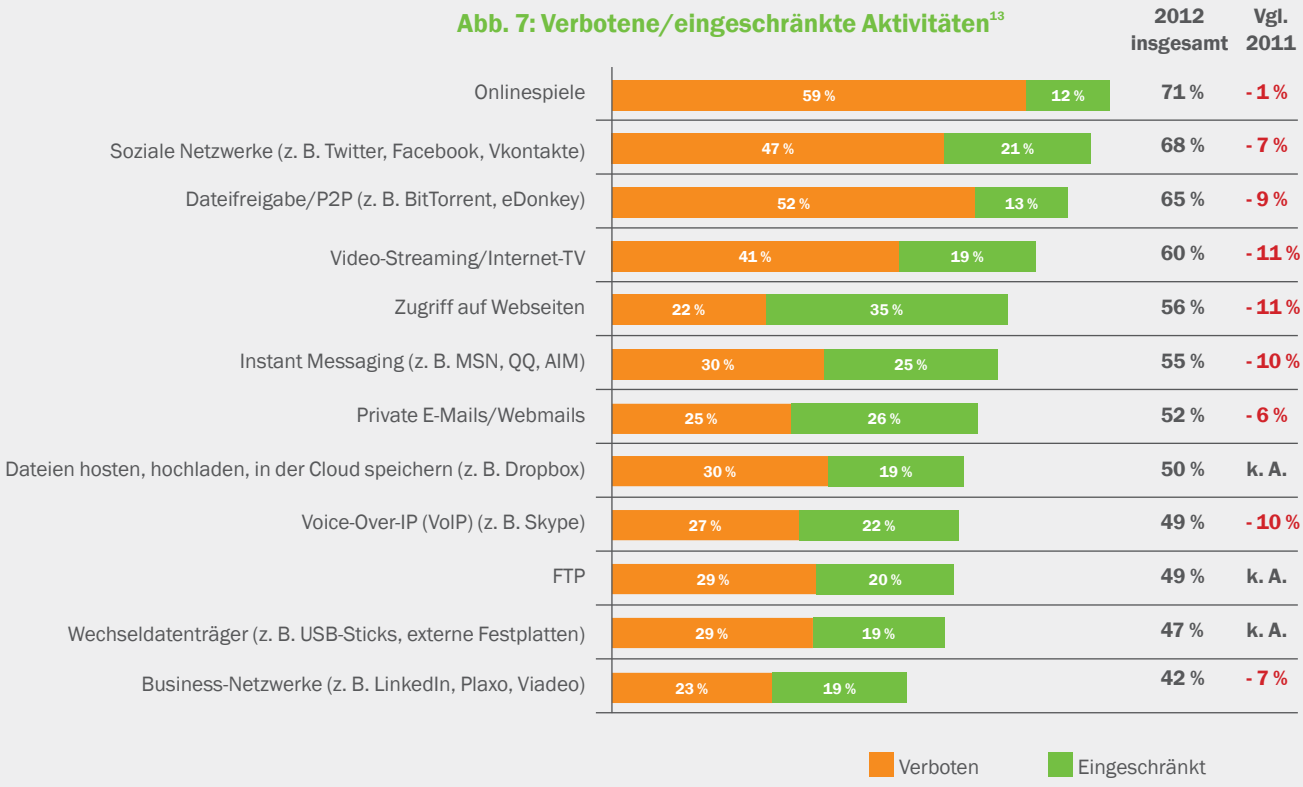
IT-Administratoren haben richtig erkannt, dass die größten Sicherheitsrisiken nicht von den Technologien ausgehen, sondern von den Anwendern selbst. Die weitverbreitete Nutzung Sozialer Netzwerke und des Internets sowie der Drang des Menschen, immer auf dem neuesten Stand zu sein, erschweren es IT-Teams, Sicherheitsrisiken zu handhaben.

10 Quelle: Bericht aus dem 2. Q. 2012 von Securelist.com: http://www.securelist.com/en/analysis/204792239/IT_Threat_Evolution_Q2_2012
11 Quelle: Weltweite Umfrage zu IT-Risiken 2012 von Kaspersky Lab
12 Quelle: https://www.lookout.com/resources/reports/mobile-lost-and-found/billion-dollar-phone-bill

Das dringlichste Problem sind Soziale Netzwerke. Ihre Nutzung gilt als größtes Risiko für die IT-Sicherheit und wird am zweitstärksten überwacht. Knapp 50 % der Unternehmen haben sie sogar gänzlich verboten (Abb. 7). Die Einschränkungen zur Nutzung Sozialer Netzwerke und des Internets werden immer weniger, und es ist schwer zu erkennen, ob dies daran liegt, dass die IT den Kampf allmählich verliert oder weil die Vorteile, die Unternehmen aus der Nutzung Sozialer Netzwerke und des Internets ziehen, überwiegen.

David Emm, Senior Regional Researcher bei Kaspersky Lab sagt dazu: *„Die Nutzung Sozialer Netzwerke komplett zu untersagen, ist gänzlich unmöglich. Sinnvoller ist, zu lernen, wie damit umzugehen ist."*[14]

Abb. 7: Verbotene/eingeschränkte Aktivitäten[13]



Es ist jedoch erschreckend, dass Unternehmen eben nicht gelernt haben, wie damit umzugehen ist. Unternehmen, die in Zukunft gut geschützt sind, werden sich insbesondere dadurch auszeichnen, die Nutzung Sozialer Netzwerke zu koordinieren und der uneingeschränkten Internetnutzung Einhalt zu gebieten. Dies liegt weniger an den mit Sozialen Netzwerken einhergehenden Risiken, sondern eher daran, dass Anwender auf in Sozialen Netzwerken eingebundene Adware und Umfragen klicken, sowie an dem generell um sich greifenden Trend, sämtliche Inhalte mit anderen austauschen zu müssen. FTP-Webseiten, Dateihosting und Uploads bergen etliche ernstzunehmende IT-Sicherheitsrisiken, werden aber von vielen Anwendern als zuverlässig und sicher erachtet.

IT-Abteilungen müssen Ausmaß und Schweregrad dieser neuen Gefahren sowie ihre Verbreitung bei Endanwendern erkennen. Nur dann können Unternehmen aller Größen ihre derzeitige Sicherheitslage und Herangehensweise objektiv beurteilen.

13 Quelle: Weltweite Umfrage zu IT-Risiken 2012 von Kaspersky Lab
14 Quelle: Weltweiter Bericht über IT-Risiken 2012 von Kaspersky Lab

Mit nur einer Plattform alles vereinfachen

4.0

Viele Programme, viele Lösungen: Unternehmen zu schützen, ist komplex

- 44 % schützen vertrauliche Daten jetzt durch Verschlüsselung.
- 33 % lassen einen unkontrollierten Netzwerkzugriff durch Smartphones zu.[15]

4.1 Warum die IT-Sicherheitsbranche für zusätzliche Erschwernis sorgt
Bisher hat es die IT-Sicherheitsbranche den Unternehmen nicht gerade leicht gemacht. Auf die Etablierung verschiedener Technologien wurde bis dato nur mit gezielten Lösungen reagiert. Das ist so nicht unüblich und zeigt nur, dass sich Markt und Technologien herausbilden.

In Unternehmen ohne eigenes IT-Sicherheitsteam klagen die mit zahlreichen Aufgaben betrauten IT-Mitarbeiter über enorm frustrierende Erfahrungen mit dem Branchenangebot. Genau das zu finden, auszuwerten und einzukaufen, was wirklich gebraucht wird, ist an sich schon eine komplizierte Angelegenheit.

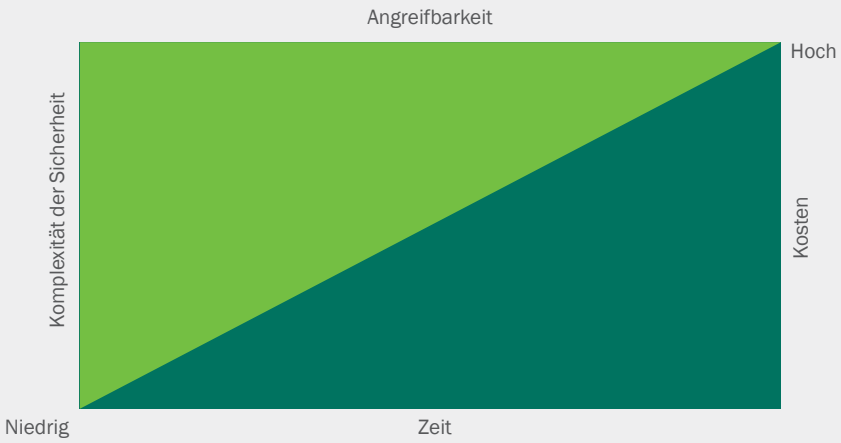
Unternehmen nutzen oft herkömmliche Anti-Malware, um wichtige Endpunkte zu schützen. Eventuell werden E-Mail- und Dateifreigabesysteme mit Verschlüsselungsfunktionen ergänzt. Wenn es mobile Endanwender gibt, haben sie mitunter in Technologien zur Verwaltung mobiler Geräte investiert, um den Zustrom von privaten und vom Unternehmen finanzierten Geräten kontrollieren und eindämmen zu können. Hinzu kommt eine bestimmte Vorgehensweise beim Patch-Management, d. h. bei der Verfolgung und Verteilung von Software-Patches in den Betriebssystemen, um Sicherheitslücken in Programmen zu schließen.

Investitionen wurden also durchaus unternommen, allerdings ist ein viel größeres Problem entstanden.

Sicherheitssysteme kommunizieren nicht miteinander. Immer, wenn ein Systemadministrator einen Bericht erstellt, eine Änderung durchführt, auf einen Alarm reagiert oder Software aktualisiert, muss für jedes Programm eine andere Managementkonsole genutzt werden. Diese manuelle Koordination von Technologien, die eigentlich miteinander verbunden sein sollten, ist ineffizient und kostet viel Zeit (Abb. 8). Einer optimalen Sicherheit steht sie obendrein im Wege.

Wenn Sie beispielsweise fünf verschiedene Sicherheitsanwendungen nutzen und es pro Anwendung fünf Minuten dauert, um auf der jeweiligen Plattform eine einzige Funktion durchzuführen, sind insgesamt 25 Minuten erforderlich. Hinzu kommt der Aufwand, der zur Überprüfung der Funktionsimplementierung entsteht. Da sich auch die Berichterstellungsverfahren der einzelnen Programme unterscheiden, kostet auch dies viel Zeit. Folglich verbringt der Sicherheitsadministrator Stunden damit, sich durch Berichte und Bildschirme zu arbeiten, um Funktionen anzuwenden, die im Prinzip automatisch erfolgen sollten.

Abb. 8: Komplexität erschwert die Sicherheit. Je komplexer die Sicherheitstechnologien sind und je länger Änderungen dauern, desto höher sind die Sicherheitskosten und desto niedriger ist die Rendite der Sicherheitsinvestitionen.[16]



15 Quelle: Weltweite Umfrage zu IT-Risiken 2012 von Kaspersky Lab 2012
16 Quelle: 2112 Group: Komplexität erschwert die Sicherheit. Oktober 2012.

„Neben dem fehlenden Know-how und der schlechten Reaktionsfähigkeit gibt es in vielen Unternehmen auch auf Betriebsebene Schwachstellen in Form verschiedener Sicherheitslösungen und Richtlinien, die für verschiedene Anwendergruppen und Geräte gelten. All dies sind mögliche Gefahrenstellen. Unternehmen müssen daher ganzheitlich vorgehen und auf eingebundene Kontrolllösungen setzen.
Chris Christiansen
VP Security Products and Services bei IDC[17]

Zwar ist Integration innerhalb der IT überstrapaziert, gerade aber zur Verbesserung der Sicherheit ist sie entscheidend. Knapp besetzte IT-Teams sind nicht in der Lage, mehrere Systeme zu verwalten, verschiedene Dashboards zu überwachen und dann noch Korrekturmaßnahmen einzuleiten.

Insbesondere bei der IT-Sicherheit zählen schnelle Erkennung und Reaktion. Je länger in einer Netzwerkumgebung Programme ohne Patch bleiben, desto höher ist ihr Gefährdungsgrad. In den heutigen komplexen Umgebungen mit ihren mobilen Geräten, virtuellen Computern und Privatgeräten von Mitarbeitern erhöht sich dieses Risiko noch. Daher ist es entscheidend, dass Änderungen schnell und einfach erfolgen können.

Das Prinzip der Integration ist in diesem Zusammenhang insofern problematisch, da bei vielen konsolidierten Ansätzen die verschiedenen individuellen Lösungen lediglich miteinander verknüpft wurden. Zwar funktionieren die Technologien miteinander, der Prozess ist aber nicht nahtlos. Außerdem ist der zeitliche Aufwand zu groß. Die Einarbeitung in die verschiedenen Schnittstellen und die Sicherstellung, dass Richtlinien in den diversen miteinander verbundenen Technologien auch durchgehend umgesetzt werden, dauert sehr lange.

Zeit ist entscheidend, und viele bereits unter Druck stehende IT-Teams haben schlichtweg nicht mehr davon. Erforderlich wäre es, mehrere Aufgaben in diversen Umgebungen von einer zentralen Stelle aus erledigen zu können.

17 Quelle: Weltweiter Bericht über IT-Risiken 2012 von Kaspersky Lab

Was nicht sichtbar ist, kann auch nicht geschützt werden: mit vereinfachter Verwaltung zu mehr Transparenz

5.0

5.1 Kosten und Ressourcen
Da Unternehmen immer mehr verschiedene Technologien anwenden, verstärkt auf Mobilität und Zusammenarbeit setzen und sich im Hinblick auf einen durchgehenden Betrieb und die Produktivität auf datengestützte Vorgänge verlassen, sind die Verbesserung der Sicherheit und die Reduzierung von Sicherheitslücken unerlässlich. Leider entsprechen die Sicherheitsanforderungen dabei nicht den Ressourcen, und größere IT-Ausgaben führen nicht notgedrungen zu mehr Personal und mehr Kompetenz.

Anbieter von IT-Sicherheitslösungen versuchen, Programme und Tools zu entwickeln und anzubieten, die besser miteinander funktionieren und sich leichter einbinden lassen. Große Unternehmen erreichen dies bereits heute mit angepassten Systemen, welche die Berichterstellung standardisieren. Dies ist allerdings extrem teuer und bedingt interne Experten zur Betreuung dieser Systeme. Für die meisten kleinen Unternehmen ist dies daher keine Option.

5.2 Neue Wege gehen und alle Endpunkte zentral einsehen, kontrollieren und schützen
Zukünftige Herangehensweisen müssen auf eine einzelne Plattform setzen, von der aus IT-Administratoren Unternehmen und Daten zentral und transparent einsehen, verwalten und schützen können.

Transparenz ermöglicht Kontrolle, und Kontrolle ermöglicht Schutz.

Besonders für kleine und mittelständische Unternehmen muss eine solche Lösung mit einem geringen Verwaltungsaufwand einhergehen, darf keine Systemintegration erfordern und muss auch von Mitarbeitern anwendbar sein, die keine IT-Sicherheitsexperten sind. Trotzdem muss es mit dieser Lösung möglich sein, alle Endpunkte, an denen auf Unternehmensdaten zugegriffen wird, nahtlos einzusehen, zu kontrollieren und zu schützen und zwar unabhängig davon, ob es sich um Desktops, virtuelle Computer, Tablet-Computer, Smartphones oder die Privatgeräte von Mitarbeitern handelt.

Grundlage der Lösung muss eine einzige und konsistente Managementkonsole sein. So lassen sich die Sicherheitstools auf einem zentralen Dashboard aufrufen und steuern, und Konfiguration, Bereitstellung, Richtlinienverwaltung und Sicherheitseinstellungen sind im gesamten Unternehmen einheitlich.

Fazit

6.0

Vorteile von Kaspersky Endpoint Security for Business:

- Anti-Malware
- Datenverschlüsselung
- Sicherheit und Verwaltung mobiler Geräte
- Kontrolle von Programmen, Geräten und Webseiten
- Systems Management und Patch Management

Kaspersky Lab weiß, dass der Schutz und die Verwaltung von Computern in den meisten Unternehmen aufwendiger und schwieriger geworden sind. Der Komplexität kann aber nur durch einen konsolidierten Ansatz bei der IT-Sicherheit Einhalt geboten werden. Die in diesem Whitepaper aufgezeigten Anforderungen und Probleme haben Kaspersky Lab angeregt, einen neuen Ansatz zu entwickeln: Kaspersky Endpoint Security for Business.

Kaspersky Endpoint Security for Business unterscheidet sich erheblich von anderen Angeboten auf dem Markt, da es grundlegend neu entwickelt wurde. Das heißt, dass anstelle mehrerer miteinander verbundener Softwarelösungen nur eine einzige IT-Sicherheitsplattform verwendet wird.

Das Ergebnis ist ein weitaus einfacheres Sicherheitsmanagement, da Richtlinien nur einmal festgelegt und dann per Mausklick auf mehreren Endpunkten und in verschiedenen Umgebungen angewendet werden können.

Kaspersky Endpoint Security for Business beinhaltet eine komplette und vollständig eingebundene Plattform mit dem vielfach ausgezeichneten Malware-Schutz, zuverlässigen Tools zur Programmkontrolle, Systems Management, Datenverschlüsselung und Verwaltung mobiler Geräte von einer einzigen Konsole aus. So können Sie Daten schützen, Programme verwalten und sämtliche Geräte einsehen, kontrollieren und schützen – ganz gleich, ob es physische, virtuelle oder mobile Geräte, Unternehmens- oder Privatgeräte sind.

Unternehmen können so endlich ein hohes Maß an Sicherheit in einer komplexen und sich häufig ändernden IT-Umgebung realisieren und zwar ohne großen Schulungsaufwand oder spezielles Know-how. Technologien, die einst als komplex, teuer und schwer zu verwalten galten, stehen jetzt allen Unternehmen unabhängig von ihrer Größe oder den verfügbaren Ressourcen zur Verfügung.

See it, control it, protect it. Now you can with Kaspersky Endpoint Security for Business

Über Kaspersky Lab

Kaspersky Lab ist das weltweit größte privat geführte Unternehmen für Lösungen zum Schutz von Endpunkten. Das Unternehmen gehört international zu den vier Spitzenanbietern für Sicherheitslösungen für Endpunktanwender. Seit seiner Gründung vor 15 Jahren liefert Kaspersky Lab Innovationen für die IT-Sicherheit und gibt Verbrauchern, kleinen und mittelständischen Unternehmen sowie großen Firmen digitale Sicherheitslösungen an die Hand. Das Unternehmen ist derzeit in nahezu 200 Ländern tätig und schützt über 300 Millionen Benutzer.

Weitere Informationen erhalten Sie unter www.kaspersky.de/business-security.