

Whitepaper
Populäre
Security-Irrtümer

Wie IT-Abteilungen unwissentlich
Cyberkriminalität fördern

KASPERSKY Lab

**SOLID
BUSINESS
PROTECTION**
BUILT THE RIGHT WAY

www.kaspersky.de

Inhaltsverzeichnis

▶ Populäre Security-Irrtümer.....	3
▶ 1. Irrtum: Daten lassen sich im Rechenzentrum isolieren.....	4
▶ 2. Irrtum: Daten auf mobilen Geräten sind nicht viel wert.....	5
▶ 3. Irrtum: Laptops und mobile Geräte sind Firmeneigentum, das nicht privat genutzt wird – somit gelangen auch Firmendaten niemals auf Privatcomputer...	6
▶ 4. Irrtum: In Sozialen Netzwerken ist man sicher.....	7
▶ 5. Irrtum: Antiviren-Software ist Massenware.....	8
▶ 6. Irrtum: Das Risikobewusstsein ist groß genug.....	9
▶ 7. Irrtum: Alle Sicherheitsverstöße sind bekannt.....	10
▶ 8. Irrtum: Richtlinien kann blind vertraut werden.....	11
▶ 9. Irrtum: Es gibt keinen Grund zur Sorge.....	12

Populäre Security-Irrtümer

Wir hoffen, dass Sie das Whitepaper „Angriffsziel Endpoint“ von Kaspersky Lab bereits gelesen haben. Falls Sie noch keine Gelegenheit dazu hatten, empfehlen wir, zuerst dieses Whitepaper herunterzuladen und zu lesen. „Angriffsziel Endpoint“ befasst sich mit dem Hauptangriffsziel der heutigen Cyberkriminellen – dem Endpunkt beziehungsweise dem Mitarbeiter.

Das vorliegende Whitepaper befasst sich damit, wie IT-Abteilungen unwissentlich und aufgrund einer Reihe falscher Annahmen und Irrtümer der Cyberkriminalität Tür und Tor öffnen und den Zugriff auf Systeme und Daten ermöglichen.

Die Nachfrage von Anwendern nach Zugang zum Internet und den neuen Kommunikationswegen ist auf einem historischen Höchststand. Auch Unternehmen haben immer höheren Bedarf an neuen Kommunikationswegen. Doch je mobiler Mitarbeiter und Unternehmensdaten werden, desto größer ist auch die Herausforderung, der drohenden Gefahr durch Cyberkriminalität Herr zu werden.

Tatsächlich werden viele IT-Abteilungen oftmals unfreiwillig und ohne ihr Wissen zu Komplizen von Cyberkriminellen. Das vorliegende Dokument zeigt auf, wie Cyberkriminelle von IT-Abteilungen in Unternehmen begünstigt werden. Außerdem werden Richtlinien vorgestellt, die dieser Praxis einen Riegel vorschieben.

Im Folgenden werden die populärsten Irrtümer erörtert, durch die IT-Abteilungen Cyberkriminellen in die Hände spielen. Ferner wird anhand von Untersuchungen Dritter und Analysen von Kaspersky-Experten erläutert, wie sich diese Fehler vermeiden lassen.

Wie steht es um die folgenden gängigen Irrtümer in Ihrem Unternehmen?

1. Irrtum: Daten lassen sich im Rechenzentrum isolieren.

Die meisten Führungskräfte greifen über ihre Smartphones (iPhone, BlackBerry und so weiter) auf ihre E-Mails zu. Eine zweite Kopie der E-Mails liegt auf ihren Laptops und eine Dritte auf den Mailservern des Unternehmens.

Insgesamt befinden sich also doppelt so viele Daten außerhalb des Rechenzentrums wie innerhalb. Hinzu kommen unzählige USB-Memory-Sticks, CDs, Sicherungsbänder, Cloud-Lösungen sowie der Datenaustausch mit Geschäftspartnern. Der Umfang, in dem Daten im Umlauf sind, ist erheblich größer als erwartet.

Obwohl wir im Grunde wissen, dass der Datenaustausch nicht eingrenzbar ist, verhalten sich IT-Abteilungen so, als sei dies möglich. Warum sonst wird unverhältnismäßig viel Zeit und Geld für die Sicherung von Rechenzentren durch Technologien wie Authentifizierung, Zugriffsverwaltung, Firewalls, Network Intrusion Prevention und so weiter aufgewendet?

Das heißt nicht, dass diese Technologien nicht wichtig wären. Im Gegenteil. Allerdings dürfen wir dabei den Ort nicht vergessen, an dem sich Daten heute vor allem befinden, nämlich am Endpoint.

Daten lassen sich nicht in Silos isolieren. Sie sind außerhalb des Rechenzentrums frei im Umlauf. Eine IDC-Studie zeigt, dass Desktops und Laptops im Hinblick auf Data Loss Prevention (DLP) als besonders problematisch gelten. Am Endpunkt besteht unmittelbar die Gefahr des Datenverlusts. Die Ergebnisse von IDC zeigen außerdem, dass bei neuen Ausgaben für Sicherheit Mobilität der wichtigste Faktor ist. Offensichtlich entwickeln immer mehr Unternehmen ein Problembewusstsein und verstärken ihre Sicherheitsvorkehrungen auch jenseits ihres Rechenzentrums.

2. Irrtum: Daten auf mobilen Geräten sind nicht viel wert.

Zeit ist Geld. Unzählige Stunden werden darauf verwendet, Berichte zu verfassen und Analysen zu erstellen, damit fundierte Entscheidungen getroffen werden können. Auch an den Wochenenden stehen neben E-Mails und Präsentationen sorgfältige Prüfungen von Geschäftschancen an, die keinen Aufschub dulden. All dies führt dazu, dass beträchtliche Datenmengen auf mobilen Geräten gespeichert werden.

Viele IT-Abteilungen behandeln einen Laptop wie einen leeren Aktenkoffer. Wird ein Gerät gestohlen oder geht es verloren, spielt für Versicherungen nur der Wert des leeren Koffers eine Rolle. Die wertvollen Daten, die auf dem Gerät gespeichert waren, werden außer Acht gelassen.

Dies erklärt auch, weshalb die Schutzmaßnahmen für mobile Geräte in der Regel auf den Wert des Geräts und nicht auf den der Daten ausgerichtet sind. Tatsache ist aber, dass der Wert der Daten oft viel größer ist als der Wert des Geräts – nicht selten um ein Hundertfaches.

Der Einsatz verwalteter Antiviren-, Diebstahlschutz- und Datenschutztechnologien für mobile Geräte ist ein erster wichtiger Schritt, um mobile Daten zu schützen.

Es gibt einen Trend in Unternehmen, vor allem Führungskräften beim Kauf geschäftskritischer mobiler Geräte wie Laptops und Smartphones die Wahl des Modells selbst zu überlassen.

Das zeigt sich exemplarisch an der wachsenden Zahl von iPhones in Unternehmensnetzwerken. Leider steht für die meisten Geschäftsleute und IT-Abteilungen der Wert des Geräts und der Zeitaufwand im Verlustfall im Vordergrund, nicht der Wert der Daten auf dem Gerät.

Mitarbeiter sind mit ihren persönlichen Lieblingsgeräten ausgerüstet, nicht mit Geräten, die für verwaltete Antiviren-, Diebstahlschutz- und Datenschutztechnologien optimiert sind. Das Ergebnis ist eine wachsende Vielzahl von Geräten, Betriebs- und Kommunikationssystemen, Sicherheitsprofilen und anderen Technologien innerhalb des Unternehmensnetzwerks.

Die Aufgabe, plattformübergreifend Sicherheit zu gewährleisten, kann Unternehmen mit kleinen Sicherheitsabteilungen schnell überfordern.

3. Irrtum: Laptops und andere mobile Geräte sind Firmeneigentum, das nicht privat genutzt wird – somit gelangen auch Firmendaten niemals auf Privatcomputer.

Noch vor wenigen Jahren wurden Unternehmensnetzwerke durch eine feste Außengrenze definiert. Durch Schutztechnologien wurde eine klare Trennlinie zwischen der Innen- und Außenseite des Netzwerks gezogen – wie ein Graben um eine mittelalterliche Burg. Externe Geräte wurden als nicht vertrauenswürdig eingestuft, Geräte im Innenbereich wurden von der Firewall des Unternehmens geschützt – wie von den Mauern einer Burg.

Viele Unternehmen weltweit profitieren davon, verstärkt auf außerhalb tätige und mobile Mitarbeiter zu setzen. Durch die Fortschritte der Mobiltechnologie können Mitarbeiter im Prinzip immer online sein und auch auf Reisen an jedem Ort weltweit vollen Zugriff auf wichtige Unternehmensressourcen haben, zum Beispiel auf Anwendungen, Dokumente und E-Mails.

Der Zugriff ist auch über mobile Handgeräte möglich. So greifen mobile Mitarbeiter auf Unternehmensnetzwerke und Daten zu, während sie sich in Flughafenlounges, Hotelzimmern oder Flugzeugen mit Internetzugang befinden. Dabei sind all diese Verbindungen unsicher. Zudem beginnen Arbeitszeiten nicht mehr um 9 Uhr und enden um 17 Uhr. Menschen arbeiten im Prinzip rund um die Uhr, greifen auf aktuelle Informationen zu, beantworten umgehend Kundenanfragen und übernehmen eine Vielzahl zusätzlicher täglicher Aufgaben.

Allerdings ergeben sich aus dieser Verfügbarkeit auch neue Schwachstellen, die zum Einfallstor für neue Angriffe werden können (Quelle: Mobile Security – IDC.)

Desktopcomputer, die ausschließlich im Büro genutzt werden, sind weniger gefährdet als mobile Geräte und nicht zwingend auf Technologien wie eine individuelle Firewall angewiesen. Für Laptops hingegen sind situationsgebundene Lösungen unerlässlich. Sobald Laptops die relative Sicherheit des Unternehmensnetzwerks verlassen, sollten erweiterte Sicherheitsfunktionen automatisch aktiviert werden. Sicherheitsvorkehrungen, etwa eine Firewall, die Deaktivierung von drahtlosen, etwa Bluetooth-Verbindungen ohne Passwortschutz und die strengere Prüfung von USB-Geräten sollten automatisch wirksam werden, sobald der Laptop das Unternehmensnetzwerk verlässt.

4. Irrtum: In Sozialen Netzwerken ist man sicher.

Soziale Netzwerke sind nicht mehr wegzudenken. Die neue Technologie ist ein Muss und einige Bereiche Ihres Unternehmens benötigen sie für ihr Wachstum. Noch vor zehn Jahren standen IT-Abteilungen vor der Aufgabe, für Internetzugang zu sorgen. Dann kamen E-Mail-Konten für Unternehmen, später Instant-Messaging-Anwendungen. Jede dieser Technologien erwies sich letztlich als wichtiges geschäftliches Tool. Soziale Medien sind lediglich der nächste Schritt. Es ist ratsam, sich auf diese neue Herausforderung einzustellen. Viele Unternehmen beschäftigt die Frage, wie sie ihren Mitarbeitern die verantwortungsbewusste Nutzung von Web-2.0-Tools gestatten können, ohne zu große Sicherheitsrisiken einzugehen oder die Einhaltung von Richtlinien zu gefährden. Durch auf sichere Weise eingesetzte soziale Medien und Web-2.0-Technologien können Unternehmen die Zusammenarbeit und Produktivität verbessern und den Umsatz steigern.

Im Mittelpunkt sollte dabei die Frage stehen, wie Unternehmen soziale Medien auf sichere Weise nutzen können, denn ein grundsätzliches Verbot wird sich, von wenigen Ausnahmen abgesehen, als nicht praktikabel erweisen.

Formelle Richtlinien zur Regelung des Zugriffs und der Verwaltung sozialer Medien sind dabei entscheidend. Ein Beispiel: Wenn ein Unternehmen sein Netzwerk zwar vor Malware-Angriffen schützt, es aber versäumt, für eine angemessene Kontrolle des Zugriffs auf Soziale Netzwerke zu sorgen, kann die Nachlässigkeit eines einzigen Mitarbeiters dazu führen, dass das Netzwerk mit Malware infiziert wird und beträchtliche direkte oder indirekte wirtschaftliche Schäden entstehen. Soziale Netzwerke sind auch mögliche Plattformen für Informationslecks durch Mitarbeiter, die freiwillig Informationen an Dritte weitergeben.

Mit Ausnahme weniger, stark kontrollierter universitärer Umgebungen ist ein Verbot sozialer Medien langfristig nicht praktikabel. Viel realistischer ist der Ansatz, Technologien einzusetzen, die den Datenaustausch mit Sozialen Netzwerken genau überwachen und schädliche Webseiten blockieren.

5. Irrtum: Antiviren-Software ist Massenware.

Umfassende Sicherheitsmodelle beruhen auf dem Zusammenspiel zahlreicher Funktionen. Die Grundfunktionen sind Schutz, Erkennung und Reaktion. Antiviren-Software wird in ihrer Wichtigkeit oft unterschätzt und als Massenware angesehen, die jährlich automatisch erneuert wird. Das führt dazu, dass die Qualität der Erkennungs- und Reaktionsfunktionen ebenfalls unbeachtet bleibt. Wie wir gezeigt haben, sind diese Elemente aber von zentraler Bedeutung für jede Sicherheitsstrategie. Es gibt ein immenses Spektrum an Lösungen für Schutz, Performance, Handhabung, Bereitstellung und Support auf dem Markt.

Viele Unternehmen sind darauf bedacht, zu neueren Technologien (zum Beispiel Data Leak Prevention, Verschlüsselung und so weiter) zu wechseln. Dies sind zweifellos hilfreiche Tools – dennoch steigt die Zahl der Malware-Vorfälle und Infektionen auch weiterhin. Eine IDC-Umfrage ergab, dass 46 Prozent der Unternehmen eine Zunahme der Malware-Vorfälle und nur 16 Prozent einen Rückgang beobachten. Bei kleinen und mittleren Unternehmen (500–2.499 Mitarbeiter) fiel der Unterschied am deutlichsten aus: 44 Prozent sehen einen Zuwachs und nur 7 Prozent einen Rückgang.

Malware findet also trotz verstärkter Schutzmaßnahmen weiterhin Schlupflöcher. Darin zeigt sich, dass das Augenmerk stärker auf die Faktoren Erkennung und Reaktion gelegt werden muss. Einerseits investieren IT-Abteilungen in Schutzfunktionen für Gateways, andererseits lassen sie es zu, dass Mitarbeiter ohne angemessene Erkennungsmechanismen im Internet surfen. Durch Letztere ließe sich sicherstellen, dass kriminelle Machenschaften erkannt und wirksam unterbunden werden.

Da Cyberkriminelle speziell Endpoints ins Visier nehmen, wird gerade dort solide Erkennungs- und Reaktionstechnologie benötigt. Endpoints werden so vor Malware geschützt, mit der Cyberkriminelle Daten entwenden und finanziellen Schaden anrichten könnten.

6. Irrtum: Das Risikobewusstsein ist groß genug.

Das Risikobewusstsein und die Schulung von Anwendern sind auf jeder Stufe und in jeder Phase der Informationssicherheitsstrategie von zentraler Bedeutung. So müssen Mitarbeiter beispielsweise lernen, sich vor schädlichem Code zu schützen, sicher im Internet zu surfen, Spy- und Scareware zu meiden und im Umgang mit Anhängen Verhaltensregeln einzuhalten.

Passwortrichtlinien sind das höchste Gebot. Auch die Richtlinien zur Internetnutzung müssen unmissverständlich kommuniziert, überwacht und durchgesetzt werden.

Ein Bewusstsein über Gefahren, Auswirkungen und Verbreitungsmethoden macht Anwender wachsam und hält sie von unüberlegten Entscheidungen ab, die zu einem Befall des Endpunkts führen könnten. Regelmäßige Informationskampagnen helfen Mitarbeitern, auf dem neuesten Stand und möglichst geschützt zu bleiben.

Selbstverständlich ist es ebenso wichtig, dass alle IT-Mitarbeiter über aktuelle Gefahren und Angriffswege im Bilde sind, damit sie bei der Wahl der besten Schutztechnologie fundierte Entscheidungen treffen können.

7. Irrtum: Alle Sicherheitsverstöße sind bekannt.

Die Zahl der angezeigten Sicherheitsverletzungen ist um mehr als 23 Prozent gestiegen, und die Verluste durch Cyberkriminalität haben sich mehr als verdoppelt – doch das ist nur die Spitze des Eisbergs. Diese vom FBI veröffentlichten Zahlen sind irreführend, da Unternehmen Sicherheitsverletzungen in der Regel gar nicht zur Anzeige bringen und die Gefahr somit nicht präzise genug quantifiziert werden kann.

Unternehmen sehen von einer Anzeige ab, weil sie befürchten, dass sich solche Informationen negativ auf Aktien, den Unternehmenswert, die Marke oder ihren guten Ruf auswirken könnten.

Diese Furcht mag verständlich sein, doch die Folge ist eine verzerrte Vorstellung des Gefahrenzuwachses im Internet. Wenn Sicherheitsverletzungen nicht angezeigt werden, entsteht der falsche Eindruck, dass die Bedrohung durch Malware minimal und die Zunahme der Cyberkriminalität eine Übertreibung wäre.

Es ist für Unternehmen nur von Vorteil, zu erfahren, welche Sicherheitsverletzungen vorgefallen sind, wie dabei vorgegangen wurde und wie man sich vor solchen Angriffen schützen kann.

8. Irrtum: Richtlinien kann blind vertraut werden.

Richtlinienkonformität und IT-Sicherheit sind nicht gleichbedeutend. Viele Unternehmen sehen Malware-Schutz als Produkt an, das man einfach kauft, regelmäßig aktualisiert – und damit hat es sich. Richtlinienkonformität geht häufig mit einem Top-Down-Ansatz einher. Dabei dient meist ein starres, formales Raster als Vorgabe. Unternehmen müssen prüfen, wie sich ihre Produkte und Dienstleistungen in dieses Raster einpassen lassen.

Echte Sicherheit beginnt jedoch an der Basis. Ob Sie ein neues Softwareprodukt oder eine neue Netzwerkarchitektur für Ihr Unternehmen entwickeln, beispielsweise eine Produktarchitektur, für die Sie anfangs Aspekte wie Kommunikation, Lokalisierung, Versionen und so weiter festlegen, es sollten dabei immer auch Sicherheitsaspekte berücksichtigt werden, die von Anfang an in die Anwendung zu integrieren sind.

Die Sicherheitselemente sollten im Verlauf der Entwicklung immer wieder neu überdacht und verfeinert werden. Fehlt das Verständnis für die Komplexität von Sicherheitsfragen in der digitalen Geschäftswelt, können Richtlinien lediglich die Illusion von Sicherheit vermitteln. Compliance sollte niemals als das eigentliche Ziel gelten.

9. Irrtum: Es gibt keinen Grund zur Sorge.

Auch die sichersten Systeme werden letztendlich von Menschen bedient. In vielen Fällen führt der menschliche Faktor zu Problemen – durch einen einfachen Irrtum, mangelndes Wissen oder fehlende Erfahrung.

Aus diesem Grund sollten Mitarbeiter in Informationsmanagement geschult werden. Sie sollten wissen, wie man sich in bestimmten Situationen verhält, wie die klar definierten, unternehmensweit gültigen Sicherheitsrichtlinien umzusetzen sind und wie sie durch Sorgfalt und Vorsicht eine Malware-Infektion vermeiden können. Falls das Netzwerk bereits von Malware befallen ist, muss die richtige Vorgehensweise zur Datensicherung und Vermeidung weiterer Verluste bekannt sein.

Ziehen Sie die Möglichkeit eines Zwischenfalls in Ihrem Unternehmen ernsthaft in Erwägung. Besteht wirklich kein Grund zur Sorge? Es liegt bei Ihnen, wertvolle Daten vor dem Zugriff Krimineller zu schützen.

Zusammenfassung

Cyberkriminelle finden fortwährend Mittel und Wege, die Endpunkte von Unternehmen zu infiltrieren, Daten zu stehlen und finanziellen Schaden anzurichten. Einem Bericht von SANS.org mit dem Titel „The Top Cyber Security Risks“ zufolge verlieren Unternehmen tagtäglich enorme Beträge – und wähen sich in Sicherheit.

Nehmen Sie die Sicherheit Ihres Unternehmensvermögens in die Hand.

Kaspersky Labs GmbH
Despag-Straße 3
85055 Ingolstadt
Deutschland

www.kaspersky.de
E-Mail: salesdach@kaspersky.de
Telefon +49 (0) 841 98 189 0
Telefax +49 (0) 841 98 189 100