

# 12 SICHERHEITSPROGNOSEN FÜR 2012





Jedes Jahr um diese Zeit erörtere ich mit meinen Forschungsteams, mit welchen Bedrohungen für unsere Kunden unserer Einschätzung nach im kommenden Jahr zu rechnen ist. Diese wichtige Analyse bildet zum einen die Grundlage, auf der wir Sie darüber informieren können, worauf Sie vorbereitet sein sollten. Zum anderen bestimmt sie unsere Ausrichtung bei der Entwicklung von Produkten und Services, mit denen wir Sie vor diesen Bedrohungen schützen können.

Für das Jahr 2012 haben wir 12 Prognosen zusammengestellt, die sich in vier Hauptkategorien zusammenfassen lassen:

- Entscheidende IT Trends
- Mobile IT-Landschaft
- Bedrohungslandschaft
- Datenlecks und Datenschutzverletzungen

Gemeinsamer Nenner dieser Prognosen ist die Entwicklung hin zu immer raffinierteren Angriffen und weg vom PC-zentrierten Desktop. Die Hoffnung auf mehr Sicherheit durch neue Betriebssysteme hat sich nicht erfüllt. Das bedeutet, dass unsere Kunden im Zuge von Konsumerisierung, Virtualisierung und Cloud-Computing zunehmend auf ein datenzentriertes Modell setzen müssen, damit Sicherheit und Datenschutz wirksam sichergestellt

werden können. Und wir bei Trend Micro müssen unsere Arbeiten auf diesen zentralen Gebieten fortsetzen. Nur so können wir unsere Kunden dabei unterstützen, diesen Sicherheitsbedrohungen im Jahr 2012 die Stirn zu bieten.

Bei Trend Micro erforschen wir kontinuierlich nicht nur die Bedrohungen von heute, sondern auch die Trends von morgen - dieses Selbstverständnis spiegelt auch der Name unseres Unternehmens wider. Auf diese Weise können wir Sie dabei unterstützen, Ihre Daten und Ressourcen besser zu schützen.

Ich hoffe, dass Sie die diesjährigen Prognosen interessant und hilfreich finden - damit Sie auch im Jahr 2012 sicher und geschützt sind.

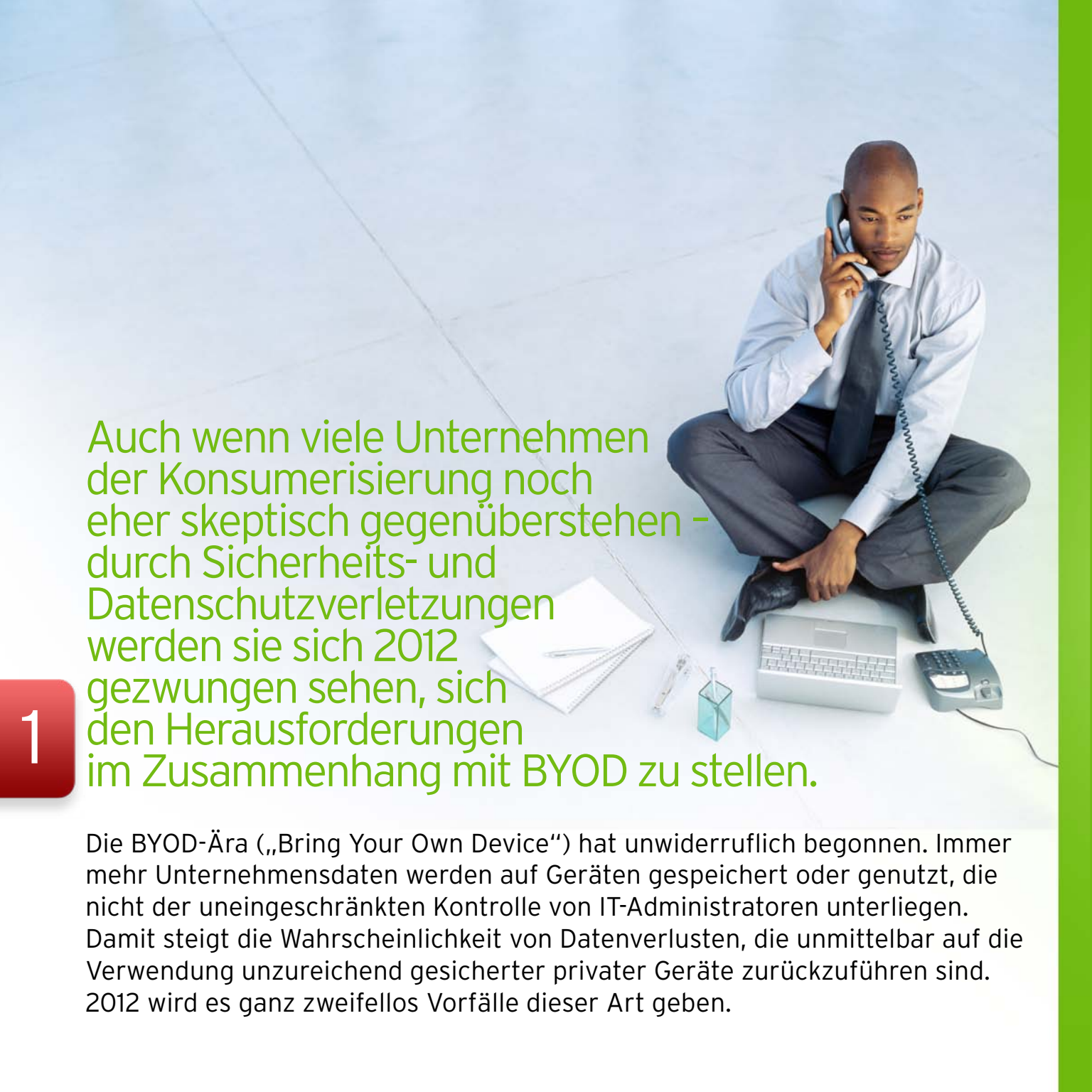
*Raimund*

Raimund Genes  
CTO, Trend Micro



# ENTSCHEI- DENDE IT-TRENDS






Auch wenn viele Unternehmen der Konsumerisierung noch eher skeptisch gegenüberstehen – durch Sicherheits- und Datenschutzverletzungen werden sie sich 2012 gezwungen sehen, sich den Herausforderungen im Zusammenhang mit BYOD zu stellen.

1

Die BYOD-Ära („Bring Your Own Device“) hat unwiderruflich begonnen. Immer mehr Unternehmensdaten werden auf Geräten gespeichert oder genutzt, die nicht der uneingeschränkten Kontrolle von IT-Administratoren unterliegen. Damit steigt die Wahrscheinlichkeit von Datenverlusten, die unmittelbar auf die Verwendung unzureichend gesicherter privater Geräte zurückzuführen sind. 2012 wird es ganz zweifellos Vorfälle dieser Art geben.

A photograph of three men in a server room. They are crouching in front of several tall server racks. The man on the left is wearing glasses and a grey shirt. The man in the middle is wearing a white shirt. The man on the right is wearing a blue shirt. They are looking towards the camera. The server racks are filled with equipment and have glass doors. The room has a greenish tint, possibly from the lighting or the server equipment.

Die eigentliche Herausforderung für Eigentümer von Rechenzentren wird darin bestehen, die immer größere Komplexität beim Schutz physischer, virtueller und cloudbasierter Systeme zu bewältigen.

2 Gezielte Angriffe auf virtuelle Maschinen (VMs) und Cloud-Computing-Services sind zwar potenziell denkbar - für Angreifer besteht jedoch keine unmittelbare Notwendigkeit zu einer solchen Vorgehensweise, da herkömmliche gezielte Angriffe auch in diesen neuen Umgebungen wirkungsvoll durchgeführt werden können. Virtuelle und cloudbasierte Plattformen sind genauso leicht angreifbar, aber schwieriger zu schützen. Die Hauptlast tragen also die IT-Administratoren, die im Zuge der Übernahme dieser Technologien dafür sorgen müssen, dass die unternehmenskritischen Daten geschützt bleiben. Das Patchen eines großen Arrays mit virtualisierten Servern stellt eine Herausforderung dar. Dabei bietet sich für Hacker die Gelegenheit, Server zu übernehmen, den Datenverkehr aufzuspalten und/oder Daten aus anfälligen Systemen zu stehlen.

# MOBILE LANDSCHAFT



A woman with blonde hair is looking down at her smartphone. She is wearing a light-colored blazer. The background is a blurred office setting with white blinds. A red square with the number 3 is on the left side of the page.

3

## Plattformen für Smartphones und Tablet-PCs, insbesondere *Android*, werden in stärkerem Maße zum Angriffsziel von Cyberkriminellen.

Mit der weltweit zunehmenden Nutzung von Smartphones werden mobile Plattformen zu immer attraktiveren Zielen für Cyberkriminelle. Besonders die Plattform *Android* hat sich zu einem bevorzugten Angriffsziel entwickelt, denn sie ist aufgrund ihres Verteilungsmodells für Apps für jedermann vollkommen offen. Wir sind davon überzeugt, dass sich dies 2012 fortsetzen wird, obgleich auch andere Plattformen unter Beschuss geraten werden.

A man in a white shirt and striped tie is holding a smartphone with a stylus. The background is a blurred office setting with light-colored blinds.

## Sicherheitslücken in mobilen Apps aus seriösen Quellen erleichtern Cyberkriminellen die Datenextraktion.

4

Bislang stammen die Bedrohungen für mobile Plattformen aus bösartigen Apps. Wir gehen davon aus, dass Cyberkriminelle es künftig auch auf Apps aus seriösen Quellen absehen werden. Voraussichtlich werden sich Schwachstellen oder auch Programmierfehler finden lassen, die einen Datendiebstahl oder -zugriff ermöglichen. Hinzu kommt, dass nur sehr wenige App-Entwickler über einen wirklich ausgereiften Prozess für den Umgang mit Schwachstellen und deren Behebung verfügen, sodass Sicherheitslücken möglicherweise über einen längeren Zeitraum bestehen bleiben.

# BEDROHUNGS- LANDSCHAFT






5

Botnetze werden zwar kleiner, ihre Anzahl nimmt jedoch zu.

Dadurch wird eine wirksame Abschaltung durch die Ermittlungsbehörden schwieriger.

Das Botnetz als „herkömmliches“ Instrument der Cyberkriminalität wird sich als Reaktion auf die Maßnahmen seitens der IT-Sicherheitsbranche weiterentwickeln. Die Tage der riesigen Botnetze könnten gezählt sein. Stattdessen wird es womöglich mehr, wenn auch kleinere, aber dadurch auch leichter kontrollierbare Botnetze geben. Durch kleinere Botnetze sinken die Risiken für Cyberkriminelle: Der Verlust eines einzelnen Botnetzes macht sich dadurch nicht mehr im gleichen Umfang für sie bemerkbar.



Hacker werden ihr Augenmerk auf neue Ziele richten. Damit geraten Systeme mit Verbindung zum Internet, die entsprechende Schwachstellen aufweisen, ins Visier – von SCADA-gesteuerten Schwermaschinen bis hin zu medizinischen Geräten.

6

Angriffe auf SCADA-Systeme zur Prozessüberwachung und -steuerung sowie sonstige Systeme, auf die über ein Netzwerk zugegriffen werden kann, werden sich 2012 häufen, denn es wird Bedrohungen durch Akteure geben, deren Interessen über den Diebstahl von Geld und wertvollen Daten hinausgehen. 2011 wurde durch STUXNET und weitere Bedrohungen deutlich, dass SCADA-Systeme zum aktiven Ziel geworden sind. Proof-of-Concept-Angriffe auf Systeme mit Netzwerkanbindung, darunter auch medizinische Geräte, werden erwartungsgemäß folgen.



7

## Cyberkriminelle werden sich kreativer vor Strafverfolgung schützen.

Cyberkriminelle werden zunehmend versuchen, Gewinne aus dem Missbrauch rechtmäßiger Online-Ertragsquellen, beispielsweise Online-Werbung, zu ziehen. Auf diese Weise bleiben sie sowohl für die Ermittlungsbehörden als auch für die von Banken und anderen Finanzinstituten zum Schutz vor Betrug eingesetzten Sicherheitswächter unsichtbar.

# DATENLECKS UND DATEN- SCHUTZVER- LETZUNGEN





## Durch weitere Hacker-Gruppen steigt die Bedrohung für Unternehmen, die hoch vertrauliche Daten in ihrem Besitz haben.

8

Online-Gruppen wie Anonymous und LulzSec haben es 2011 zu Berühmtheit gebracht, indem sie aus unterschiedlichen politischen Gründen Unternehmen und Einzelpersonen ins Visier genommen haben. Die Motivation dieser Gruppen wird 2012 aller Wahrscheinlichkeit nach noch steigen. Sie werden ihre Fähigkeiten, in Unternehmen einzudringen und die Aufspürung durch IT-Profis und Ermittlungsbehörden zu vermeiden, weiter verbessern. Unternehmen müssen sich dieser neuen Bedrohung stellen und ihre Bemühungen zum Schutz unternehmenskritischer Geschäftsdaten intensivieren.



## 9 Mit der neuen Generation der „sozialen Netzwerker“ wird Datenschutz neu definiert.

Vertrauliche Daten werden online gestellt - und zwar größtenteils durch die Nutzer selbst. Die neue Generation der jungen Nutzer sozialer Netzwerke hat eine andere Einstellung zum Schützen und Freigeben von Informationen. Persönliche Daten werden bereitwilliger an Dritte weitergegeben, beispielsweise in sozialen Netzwerken. Sie treffen aller Wahrscheinlichkeit nach keine Maßnahmen, um den Zugriff auf diese Informationen auf spezifische Gruppen, z. B. Freunde, zu beschränken. In einigen Jahren werden Datenschutzbewusste in der Minderheit sein. Damit bieten sich für Angreifer erstklassige Aussichten.



Mit der allgemeinen Verbreitung von Social Engineering werden Unternehmen zu leichten Opfern.

10

Bis dato waren die trickreichsten Manöver unter Ausnutzung von Social-Engineering-Netzwerken gegen Großunternehmen gerichtet. Cyberkriminelle sind inzwischen jedoch so versiert auf diesem Gebiet, dass der Aufwand für Angriffe auf einzelne Unternehmen für sie immer geringer wird. Dadurch und auch durch die größere Menge der online verfügbaren persönlichen Informationen können Cyberkriminelle individuellere und auf das jeweilige Ziel feiner abgestimmte Angriffe gegen Unternehmen aller Größenordnungen starten. Wie schon in der Vergangenheit werden Cyberkriminelle auch künftig ihr Hauptaugenmerk darauf richten, sich Zugang zu den Online-Bankkonten von Unternehmen zu verschaffen.

## Neue Bedrohungsakteure nutzen raffinierte Tools aus dem Bereich der Cyberkriminalität zur Verfolgung eigener Ziele.

Die Anzahl gezielter Angriffe wird 2012 weiter zunehmen. Diese Angriffe werden jedoch nicht ausschließlich von Cyberkriminellen ausgehen. Da sich komplexe, hartnäckige Bedrohungen (Advanced Persistent Threats, APT) zunehmend als wirkungsvoll erweisen, werden auch andere interessierte Parteien - etwa Aktivistengruppen, Unternehmen und Regierungen - dazu übergehen, vergleichbare Tools und Taktiken zur Erreichung ihrer Ziele einzusetzen.

12

2012 wird es weitere Aufsehen erregende Vorfälle im Zusammenhang mit Datenverlusten infolge von Malware-Infektionen und Hacker-Angriffen geben.

Auch 2012 werden große Organisationen wieder Aufsehen erregenden Angriffen zum Opfer fallen. Wichtige und vertrauliche Unternehmensdaten werden mittels Malware-Infektionen und Hacker-Angriffen extrahiert. Infolgedessen wird es zu Datenverlusten in erheblichem Umfang kommen, von der viele tausend Anwender mit ihren persönlichen Daten betroffen sein können. Diese Vorfälle können beträchtliche direkte und indirekte Schäden für die Betroffenen nach sich ziehen.





Trend Micro Incorporated, ein weltweit führender Anbieter von Cloud-Sicherheitslösungen, schafft mit Internet Content Security und Bedrohungsabwehr eine sichere Welt zum Austausch digitaler Daten für Unternehmen und Privatanwender. Als Pionier im Bereich Server-Sicherheitslösungen mit über 20 Jahren Erfahrung bieten wir client-, server- und cloudbasierte Sicherheitslösungen der Spitzenklasse, die die Anforderungen unserer Kunden und Partner erfüllen. Unsere Lösungen wehren Bedrohungen schneller ab und schützen Daten in physischen, virtualisierten und cloudbasierten Umgebungen. Mit der Unterstützung des Trend Micro™ Smart Protection Network™ - unserer branchenführenden, cloudbasierten Sicherheitstechnologie - und über 1.000 Bedrohungsexperten weltweit stoppen unsere Produkte und Services Bedrohungen dort, wo sie entstehen: im Internet. Weitere Informationen finden Sie unter [www.trendmicro.com](http://www.trendmicro.com).



Securing Your Journey  
to the Cloud