DIE WIRTSCHAFTLICHKEIT DER ABWEHR VON CYBERANGRIFFEN

Modellierung von Sicherheitsinvestitionen zu Risiken im Zeitalter zunehmender Online-Bedrohungen

JUNIPER NETWORKS

Die Wirtschaftlichkeit der Abwehr von Cyberangriffen: Modellierung von Sicherheitsinvestitionen zu Risiken im Zeitalter zunehmender Online-Bedrohungen

Die neue Studie „The Defender's Dilemma: Charting a Course Toward Cybersecurity", die von der RAND Corporation im Auftrag von Juniper Networks durchgeführt wurde, ist das erste heuristische Modell seiner Art, das Unternehmen dabei hilft, die wirtschaftlichen Triebfedern und Herausforderungen bei der Abwehr von Cyberattracken darzustellen.

Cyberangriffe werden mehr und mehr zu einem der größten Unternehmensrisiken, denen Firmen in allen Branchen ausgesetzt sind. Angefangen beim Diebstahl geistigen Eigentums durch Industriespionage bis hin zu erschreckend häufigen und umfassenden Datenschutzverletzungen; fest steht, dass Unternehmen wesentlich mehr tun müssen, um auf Angriffe und Bedrohungen vorbereitet zu sein und Risiken effektiv zu begegnen. Deswegen haben Unternehmen sehr viel Zeit, Energie und Ressourcen darauf verwendet, die Bedrohungen zu stoppen, denen sie durch diese Angriffe ausgesetzt sind.

Dieser Fokus hat einen guten Grund. Eine von Juniper Networks gesponserte Studie der RAND Corporation (RAND) „Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar" des letzten Jahres hat gezeigt, dass Angreifer Cyber-Schwarzmärkte aufgebaut haben, die mittlerweile eine bislang einmalige wirtschaftliche Reife zeigen. In der Praxis können Angreifer durch diese Märkte viel effektiver in Unternehmensnetzwerke eindringen und daraus auch einen höheren Gewinn schlagen. Tatsächlich haben Untersuchungen prognostiziert, dass die Angriffsmöglichkeiten bald die Fähigkeiten der Verteidigung überholen werden.

> Juniper ist der festen Überzeugung, dass das ökonomische Kalkül der Angreifer zwar deutlich ist, dies aber nicht gleichermaßen für Unternehmen gilt, die sich in weitaus hektischeren, chaotischeren und undeutlicheren Verhältnissen bewegen.

Schlüsselergebnisse des Berichts:

Juniper identifiziert im neuen Modell von RAND fünf wichtige Treiber, welche die Kosten der Cybersicherheit für Unternehmen beeinflussen. Diese werden in dieser Zusammenfassung und in RANDs vollständigem Bericht näher behandelt. Jeder dieser Treiber hat derzeit einen signifikanten Einfluss auf Kosten oder wird ihn in der Zukunft haben.

1. Es gibt keine Universallösung: Die Investitionsstrategien von Unternehmen sind nicht optimal
2. Viele Sicherheitstools sind nur für einen bestimmten Zeitraum nützlich und verlieren dann an Wert
3. Die Bedeutung von Mitarbeitern: Investitionenin die Belegschaft können langfristig Kosten sparen
4. Das Internet der Dinge befindet sich an einem Scheideweg
5. Das Beseitigen von Software-Schwachstellen führt zu bedeutenden Kostensenkungen

Obwohl viele Sicherheitsexperten schon seit langem wissen, dass es wichtig ist, diese Treiber als Teil eines Sicherheitsprogramms zu berücksichtigen, zeigen die Untersuchungen von RAND nun zum ersten Mal anhand von quantitativen Modellen auf, welchen Einfluss die Treiber auf die Kosten haben. Dieses neue Modell liefert datengestützte Erkenntnisse über die Bedeutung eines jeden Treibers und kann Unternehmen helfen, Sicherheitsrisiken strategisch und ganzheitlich zu begegnen.

Das Dilemma des Verteidigers

Die neue Studie von RAND betrachtet die wirtschaftlichen Bedingungen der Cyber-Abwehr und zeigt auf, dass Chief Information Security Officers (CISOs) gegen Windmühlen zu kämpfen scheinen—sie investieren viel Geld in Sicherheit, ohne sich sicherer zu fühlen. Bedenklicher ist jedoch, dass sie glauben, dass die Angreifer die Verteidiger bald eingeholt haben, und sie sich nie sicher sind, ob und wann sie genügend in die Sicherheit investiert haben.

Diese Dynamik ist teilweise damit zu begründen, dass sowohl Unternehmen als auch die Sicherheitsbranche selbst Cybersicherheit noch immer nicht als ein Unternehmensrisiko verstehen. Das Konzept der Risikoverwaltung wird in der Cybersicherheit oft falsch verstanden; man konzentriert sich auf die Risiken durch Bedrohungen und Schwachstellen anstatt auf die Risiken für Geschäftsergebnisse und -abläufe. Oftmals wird der Fokus —selbst in den Metriken, die den Wert von Sicherheitsprogrammen zeigen sollen—auf die Fähigkeit eines Tools oder Programms zur Abwehr einer bestimmten Anzahl von Angriffen gelegt, anstatt auf Metriken, die mehr Bedeutung für das eigentliche Geschäft haben.

Ein umfassendes Sicherheitsprogramm sollte nicht den Umfang der abgewehrten Angriffe zählen, sondern zum Ziel haben, die Rendite der Risikoverwaltung zu verstehen (Risikorendite), bzw. die Senkung des Risikos im Verhältnis zur Investition (Reduction of Risk on Investment - RROI). Dies bedeutet, dass man die Faktoren verstehen muss, welche die Gesamtkosten der Cybersicherheitsrisiken hauptsächlich beeinflussen, damit man diese in der Zukunft effizienter verwalten kann.

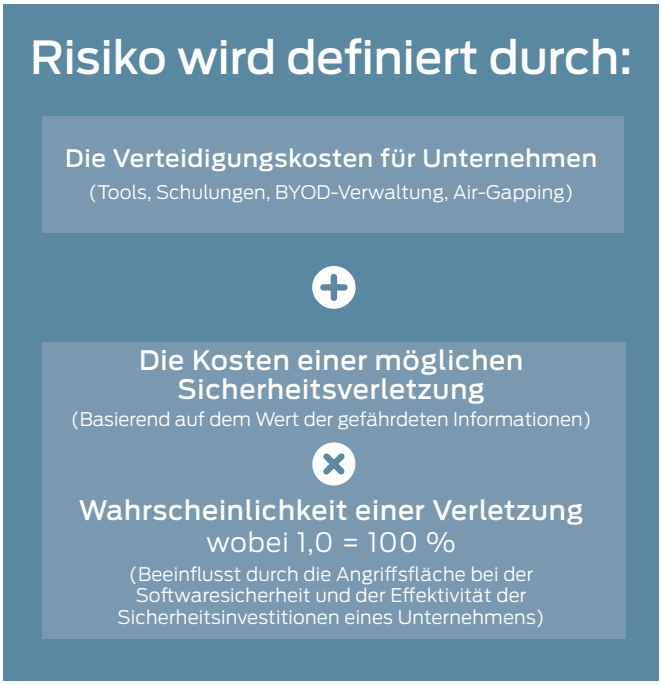
Um dieses Problem zu lösen, hat Juniper Networks eine Reihe von Wirtschafts- und Sicherheitsexperten von RAND beauftragt, die Hauptfaktoren zu untersuchen, die Kosten von Cybersicherheitsrisiken für Unternehmen beeinflussen. Diese Untersuchung betrachtet auch die Investitionen, die Unternehmen vornehmen können, um die Risiken für Reputation, Daten und Netzwerke durch die steigende Bedrohung durch Angriffe zu verwalten.

RAND hat eine nachgewiesene Erfolgsbilanz in der Bereitstellung objektiver Analysen und Erkenntnisse, die bereits in anderen Branchen im Umgang mit Herausforderungen effizient umgesetzt wurden—von der Ausgabenkontrolle im Gesundheitssektor bis hin zu Konflikten im Bereich nationaler Sicherheit und Verteidigungsausgaben. Die Untersuchung der Kosten für Cybersicherheit in Unternehmen wird sowohl der Sicherheitsbranche als auch deren Experten helfen, viele Herausforderungen, denen sie ausgesetzt sind, zu bestätigen und dies mit besseren Argumenten und Lösungsvorschlägen an die Führungsebene zu kommunizieren.

Ein ganzheitliches Modell für Sicherheitsrisiken von Unternehmen

Der Schlüssel für RANDs Bemühungen war die Entwicklung des ersten ganzheitlichen Modells, das Unternehmen ein Lerninstrument bietet, um sowohl die Hauptfaktoren besser zu verstehen, welche die Verwaltungskosten für Sicherheitsrisiken beeinflussen, als auch die verschiedenen Investitionsentscheidungen, die Kosten beeinflussen. Durch die Untersuchung, wie dieser Faktoren zusammenspielen, bietetdas Modell einen Rahmen, um in der Zukunft andersüber Entscheidungen im Bereich Cybersicherheit nachzudenken.

Obwohl bereits mehrere wertvolle Modelle zu Sicherheitsrisiken bestehen, wie ‚Operationally Critical Threat, Asset and Vulnerability Evaluation' (OCTAVE) und ‚Factor Analysis of Information Risk' (FAIR), die Unternehmen dabei helfen, die spezifischen Risiken für ihr Unternehmen und die kritischsten Daten zu bestimmen, ist RANDs Modell das erste Rahmenwerk, das die *Gesamtkosten* der Verwaltung von Cybersicherheitsrisiken darstellt. Das ganzheitliche Bild entsteht dadurch, da betrachtet wird, wie die verschiedenen Entscheidungen von Unternehmen, die Einführung neuer Technologien und die Aktionen von Angreifern miteinander im Zusammenhang stehen und sich gegenseitig sowie die Kosten für Cybersicherheit beeinflussen.



Um ein ganzheitliches Bild der Risiken zu erhalten, untersucht das Modell von RAND die verschiedenen Arten, in denen Unternehmen versuchen, die Gesamtkosten für Cybersicherheit zu minimieren. Dies betrifft sowohl direkte und indirekte Kosten, die Unternehmen bei der Abwehr von Cyberangriffen entstehen, als auch die potentiellen Verluste, die bei einem erfolgreichen Angriff entstehen könnten, die anhand des Wertes der gefährdeten Informationen und der Wahrscheinlichkeit eines erfolgreichen Angriffs berechnet werden.

> RANDs Modell ist das erste Rahmenwerk, das die *Gesamtkosten* der Verwaltung von Cybersicherheitsrisiken darstellt

Um die Kosten für ein Unternehmen zu bestimmen, verwendet das Modell von RAND 27 Parameter, welche die Kosten für ein Unternehmen in einem Zeitraum von 10 Jahren beeinflussen. Jeder Parameter kann angepasst werden, um den Einfluss auf die Kosten zu zeigen.

Die Parameter können allgemein in drei Kategorien unterteilt werden:

1. **Organisatorische Merkmale:** Die Größe des Unternehmens, die Anzahl der Computer/Geräte im Netzwerk und der Wert der gefährdeten Informationen.
2. **Sicherheitsprogramme und Investitionen:** Das Modell ermöglicht es Unternehmen, Entscheidungen über die Verwendung von vier verschiedenen Werkzeugen zu treffen, die sowohl einen Kostenfaktor beinhalten als auch die Wahrscheinlichkeit eines erfolgreichen Angriffs verringern:
   - Direkte Kosten für den Erwerb und die Verwendung von Sicherheitstools
   - Direkte und indirekte Kosten für die erweiterte Schulung des Personals zu Bedrohungen
   - Indirekte Kosten, die durch Verluste entstehen, wenn die Produktivität möglicherweise durch Einschränkungen auf Mobilgeräten wie Smartphones und besonders empfindlichen Subnetzwerken verringert wird
   - Die Gewissenhaftigkeit des Sicherheitspersonals bei der Durchführung von Sicherheitsprogrammen
3. **Veränderungen des Ökosystems:** Der Einfluss von Veränderungen im technologischen Ökosystem auf die Sicherheitskosten. Beispielsweise wie die Einführung von mehr Geräten mit dem Internet der Dinge (IoT) die Angriffsfläche verändert, oder wie die Anzahl der in einem Jahr eingeführten Software-Schwachstellen die Wahrscheinlichkeit eines erfolgreichen Angriffs beeinflusst und die daraus entstehenden Kosten

In der Praxis kann dieses Modell nach Ansicht von Juniper ein Ansatzpunkt für CISOs sein, um die verschiedenen Entscheidungen, die sie treffen müssen, um ihr Unternehmen zu schützen, besser zu verstehen und dadurch mehr Unterstützung und Mitarbeit von der gesamten Führungsebene zu erhalten.

> In der Praxis kann dieses Modell nach Ansicht von Juniper ein Ansatzpunkt für CISOs sein, um die verschiedenen Entscheidungen, die sie treffen müssen, um ihr Unternehmen zu schützen, besser zu verstehen und dadurch mehr Unterstützung und Mitarbeit von der gesamten Führungsebene zu erhalten.

Aus diesem Grund hat Juniper eine interaktive Version des Modells erstellt, die es Unternehmen ermöglicht, viele der Parameter auf ihr Unternehmen anzuwenden. Benutzer haben die Möglichkeit, die Hauptvariablen zu ändern, die den größten Einfluss auf die Kosten haben, so dass sie die optimale Mischung an Sicherheitsinvestitionen ermitteln können, die sie zukünftig in Betracht ziehen sollten.

Letztendlich sind die Vorhersagen des Modells eher richtungsweisend als analysierend, da jedes Unternehmen völlig einzigartige Anforderungen und Herausforderungen hat. Jedoch bietet es einen guten Ansatzpunkt und eine Diskussionsgrundlage für Sicherheitsexperten, die mehr Unterstützung in ihrem Unternehmen erhalten wollen.

Unternehmen und Entscheidungsträger, die dieses Modell genauer betrachten möchten, können die Methodik des gesamten Modells von RAND im Anhang des vollständigen Berichts finden.

WIRTSCHAFTLICHE ERWÄGUNGEN ZUR VERWALTUNG VON CYBERSICHERHEIT

Das Modell zeigt die Wechselwirkungen zwischen den Kosten von Cyberangriffen und den Ausgaben eines Unternehmens für Sicherheit.

KOSTEN WERDEN DEFINIERT ALS SUMME VON:

Verluste durch Cyberangriffe **+** direkte Kosten durch Schulungen **+** direkte Kosten für den Erwerb und die Verwendung von Sicherheitstools **+** indirekte Kosten im Zusammenhang mit Einschränkungen der Verwendung von BYOD Mobilgeräten **+** indirekte Kosten der Air-Gaps für empfindliche Subnetzwerke

VERLUSTE DURCH CYBERANGRIFFE

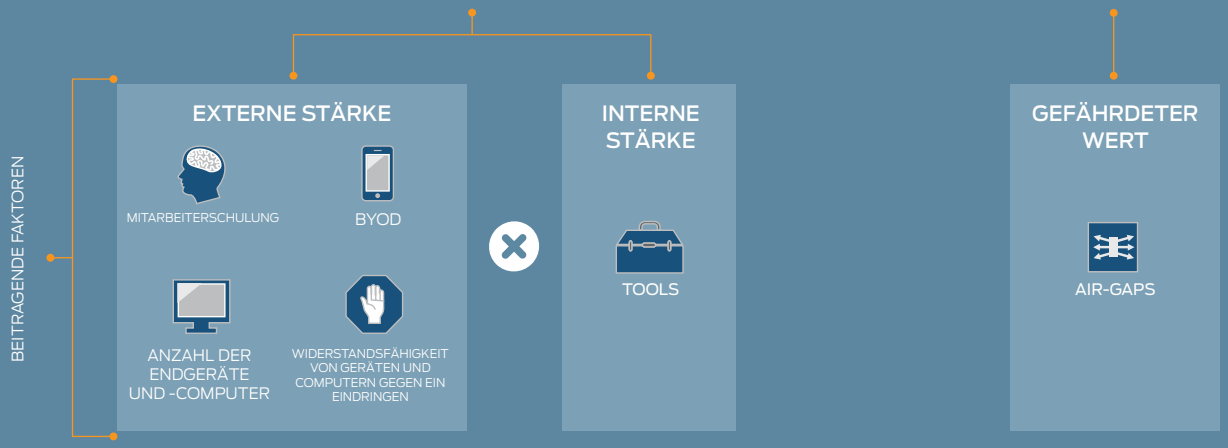
WAHRSCHEINLICHKEIT EINES ANGRIFFS

DIE WAHRSCHEINLICHKEIT ERFOLGREICHER ANGRIFFE AUF EIN UNTERNEHMEN IN EINEM BELIEBIGEN JAHR WIRD IM MODELL ALS ERGEBNIS DER EXTERNEN UND INTERNEN STÄRKEN DER ORGANISATION BETRACHTET.

×

AUSWIRKUNG DES ANGRIFFS

DIE AUSWIRKUNG EINES ERFOLGREICHEN ANGRIFFS AUF EIN UNTERNEHMEN WIRD DURCH DEN WERT DER INFORMATIONEN BESTIMMT, AUF DIE EIN ANGREIFER ZUGREIFEN KANN.



VERÄNDERUNGEN IM LAUFE DER ZEIT WAREN:

- Die Anzahl und Verletzlichkeit von Computern und Geräten
- Veränderungen in den mit Cyberangriffen verbunden Verlusten
- Die Einführung neuer Cybersicherheitstools
- Die abnehmende Wirksamkeit einiger Tools angesichts von Gegenmaßnahmen

Berechnungen wurden für das Jahr 0 durchgeführt (nehmen Sie 2015 an) und über einen Zeitraum von 10 Jahren jährlich wiederholt.

Jahr 0 ——— Jahr 10

JUNIPER NETWORKS

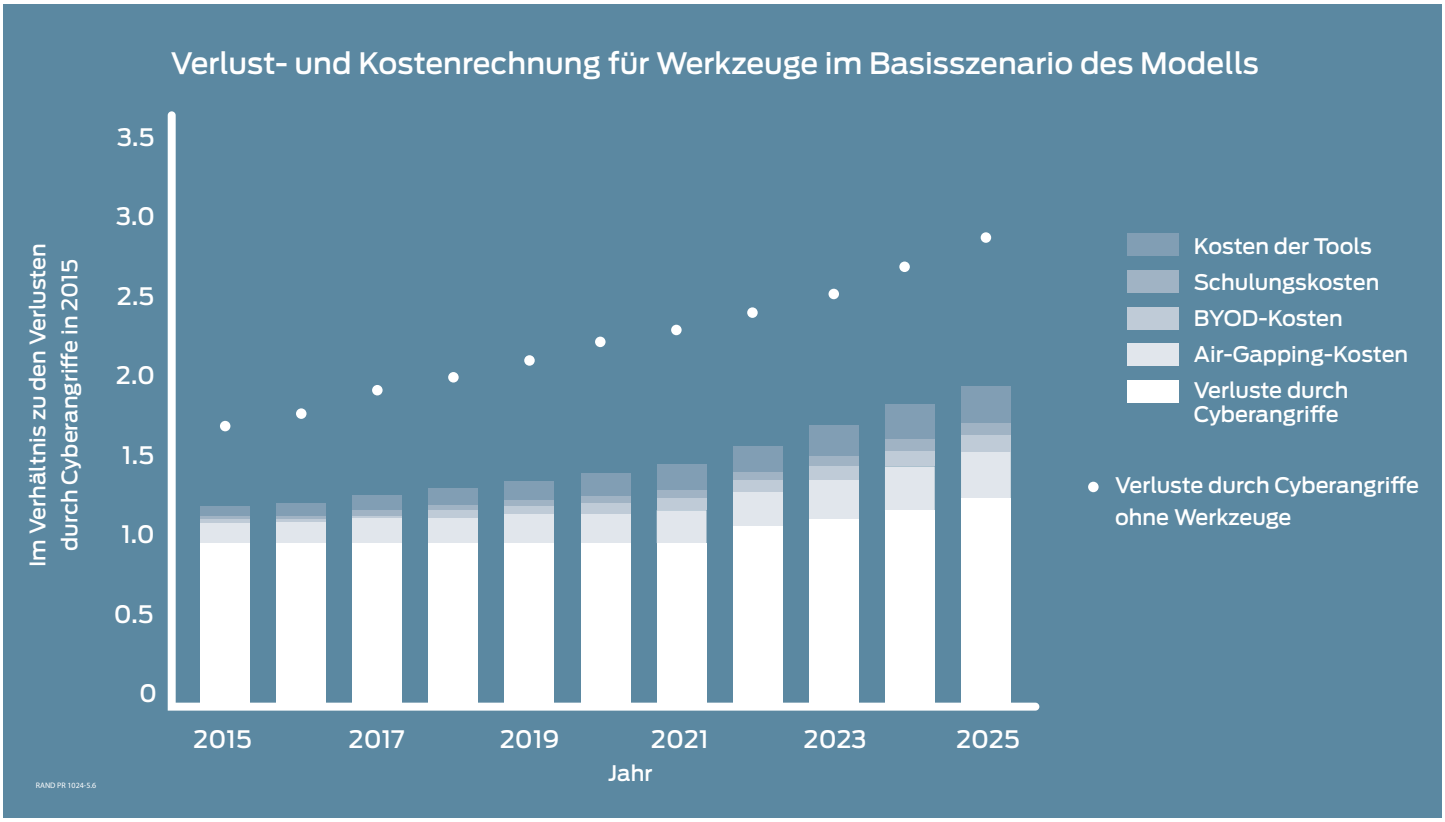
Durch das Modell erlangte Erkenntnisse über die Entwicklung im Bereich Sicherheit

Die Erkenntnisse, die aus dem Modell gewonnen wurden, sind sogar noch wichtiger als die Funktionsweise des Modells. Der Bericht von RAND wendet das Modell auf ein Basisszenario an, bei dem sowohl die Kosten in der gesamten Geschäftswelt betrachtet werden als auch derenVeränderungen in einem Zeitraum von zehn Jahren.

Im Modell von RAND wird angenommen, dass die Kosten zur Verwaltung von Cybersicherheit in den nächsten zehn Jahren in allen Unternehmen um 38 Prozent steigen werden.

> Es wird angenommen, dass die Kosten zur Verwaltung von Cybersicherheit in den nächsten zehn Jahren in allen Unternehmen um 38 Prozent steigen werden.

Auffallend ist hier, dass die Kostensteigerung nicht durch einen Anstieg der Cyberangriffe verursacht wird, sondern vielmehr durch die steigenden Kosten von Sicherheitsprogrammen (z.B. Investitionen in Tools und Schulungen, Einschränkung von ‚Bring Your Own Device' (BYOD)/Mobilgeräten und Air-Gapping von Netzwerken) für Unternehmen, wodurch sich Unternehmen vor möglichen Verlusten schützen wollen. Diese Investitionen sind letztendlich kosteneffizient, da die Verluste ohne diese Investitionen viel größer ausfallen und schneller ansteigen würden. Die gestrichelte Linie in der unteren Abbildung zeigt die Verluste, die Unternehmen erlitten hätten, wenn sie nicht in den Schutz ihrer Netzwerke investiert hätten.



Hauptsächliche Kostenfaktoren für Chief Information Security Officers

Das Modell von RAND bietet auch wertvolle Erkenntnisse für Unternehmen. Nach Ansicht von Juniper zeigt das Modell von RAND fünf hauptsächliche Kostenfaktoren auf, die Unternehmen in Betracht ziehen müssen, wenn sie ihre Sicherheitslandschaft weiterentwickeln. Viele Sicherheitsexperten kennen diese Faktoren bereits aus der Praxis, ihre große wirtschaftliche Bedeutung wird nun durch das Modell von RAND bestätigt.

1. Es gibt keine Universallösung: Die Investitionsstrategien von Unternehmen sind nicht optimal

Die Untersuchung von RAND legt nahe, dass viele Unternehmen wahrscheinlich nicht die beste wirtschaftliche Strategie im Bereich Investitionen verfolgen. Die optimale Anzahl der Sicherheitstools, Schulungen für Mitarbeiter, Einschränkungen von privaten Geräten und Entscheidungen hinsichtlich der Segmentierung von Netzwerken vom Internet sind von Unternehmen zu Unternehmen sehr verschieden.

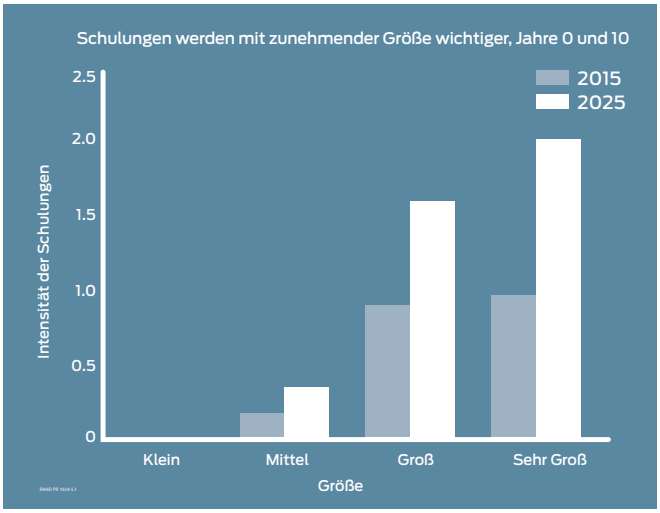
Kleine und mittelständische Unternehmen

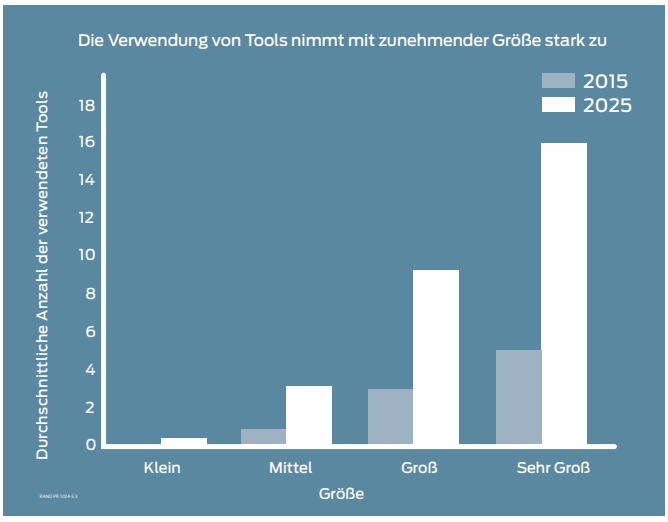
Kleine und mittelständische Unternehmen (KMU) ziehen den größten Nutzen aus einfachen Tools und Richtlinien, ohne zu viele Investitionen in komplexe Sicherheitsschulungen und erweiterte Sicherheitstechnologien zu tätigen. Da KMU eine kleinere Angriffsfläche bieten und es unwahrscheinlich ist, dass sie einen erfahrenen Angreifer abwehren müssen, würden kostspielige Sicherheitsinvestitionen in Relation zur Wahrscheinlichkeit eines Angriffs und den daraus entstehenden Verlusten unverhältnismäßig hohe Kosten verursachen. Stattdessen können bereits einfache Tools und Richtlinien KMU dabei helfen, ihr Netzwerk zu schützen und die Verwendung privater Geräte auf ihm einzuschränken.

Großunternehmen und hochwertige Ziele

Auf der anderen Seite benötigen Großunternehmen und/oder Unternehmen mit hochgradig vertraulichen Informationen, wie Rüstungsunternehmen und Unternehmen mit einem großen Umfang an geistigem Eigentum, eine ganze Bandbreite an Richtlinien und Tools. Die Wahrscheinlichkeit, dass sie einem erweiterten Angriff ausgesetzt sind, täglich eine hohe Anzahl an Angriffen abwehren müssen oder durch andere Formen des Eingriffs gefährdet sind, ist viel höher. Wenn keine bedeutenden Investitionen getätigt werden, können die Verluste durch einen solchen Vorfall immens sein.

Außerdem ist es möglich, dass Großunternehmen Vorteile aus den Skaleneffekten der Sicherheitsinvestitionen ziehen können. Beispielsweise werden erweiterte Sicherheitsschulungen pro Person kostengünstiger, wenn die Anzahl der Mitarbeiter steigt.





Unter der Annahme, dass grundlegende Schulungen zur Sicherheit und Standardtools bereits implementiert sind.

2. Viele Sicherheitstools sind nur für einen bestimmten Zeitraum nützlich und verlieren dann an Wert

Eine der größten Herausforderungen für Unternehmen sind die Gegenmaßnahmen, die Cyberkriminelle ergreifen, um die Schutzmechanismen zu umgehen. Angreifer entwickeln kontinuierlich Maßnahmen, die sie den Sicherheitstechnologien entgegensetzen, wodurch die Effektivität der Security-Tools im Laufe der Zeit abnimmt, so dass Unternehmen in neue Technologien investieren müssen.

Als Beispiel hierfür wäre Sandboxing oder Anti-Virus anzuführen. Obwohl diese Tools bei ihrer Markteinführung von hoher Bedeutung und ein wichtiger Bestandteil einer jeden Sicherheitsstrategie großer Unternehmen waren, sind sie doch anfällig für Gegenmaßnahmen. Aus diesem Grund müssen sie ständig überprüft werden. Auch sollten neue Lösungen müssen implementiert werden, um weiterhin effektiv gegen Angriffe vorgehen zu können. Maßnahmen erzeugen Gegenmaßnahmen (die Dynamik der Gegenspieler) - dies ist die Grundursache für die Entwicklung von Cybertools.

Diese Entwicklung lässt die Kosten für Sicherheitstechnologien steigern, in die Unternehmen investieren müssen, um weiterhin gut geschützt zu sein. Auch die Betriebskosten von Unternehmen erhöhen sich, da Sicherheitsexperten sie oftmals sehr komplexe und unterschiedliche Sicherheitstechnologienverwalten müssen.

Im Modell von RAND geht man davon aus, dass *die Effektivität der Technologien, die Gegenmaßnahmen ausgesetzt sind, innerhalb von 10 Jahren um 65 Prozent abnehmen wird*. Wenn man die Ausgaben des ersten mit dem des letzten Jahres im Modell vergleicht, ergibt sich eine Steigerungen des Gesamtbetrags, den Unternehmen in Sicherheitstools im Verhältnis zu den Gesamtkosten für Sicherheit investieren sollten, um 16,2 Prozent. Diese Zahl mag auf den ersten Blick zwar klein erscheinen. Zieht man jedoch in Betracht, dass Ausgaben in Security-Tools den größte Kostenfaktor für Unternehmen im Bereich Sicherheit darstellen, dann würde diese Steigerung einem signifikanten Geldbetrag entsprechen.

In welche Bereiche sollten Unternehmen demnach investieren? RAND hat auch festgestellt, dass bestimmte Arten von Sicherheitstools nicht anfällig für Gegenmaßnahmen sind. In diese Kategorie fallen Technologien und Sicherheitsfunktionen, die sich auf die Verbesserung von Sicherheits- und Patchmanagement, Automation und auf eine bessere Durchsetzung von Sicherheitsrichtlinien im gesamten Unternehmensnetzwerk konzentrieren, da diese nicht die Tools sind, die Angreifer normalerweise versuchen zu umgehen.

Letztendlich benötigen Unternehmen jedoch eine Mischung aus Tools beider Kategorien, um ihre Systeme zu schützen. Laut Juniper ist jedoch das Wichtigste, dass Unternehmen sich dieser Dynamik bewusst sind und sie bei der Einschätzung neuer Investitionen berücksichtigen.

Anfällig für Gegenmaßnahmen

- Erkennung von Unregelmäßigkeiten
- Signaturerkennung
- Sandboxing-Malware
- Hack-Backs (Gegenangriffe)
- Schulungen zu Anti-Phishing

Weniger anfällig für Gegenmaßnahmen

- Richtliniendurchsetzung und Automation bei Firewalls
- Multi-Faktor-Authentifizierung
- Automatisiertes Patch-Management und Überwachung der Patch-Versionen
- Isolierung von Subnetzwerken
- Zugriffskontrolle für Netzwerke

3. Die Bedeutung von Mitarbeitern: Investitionenin die Belegschaft können langfristig Kosten sparen

Einer der Faktoren, die laut dem RAND Modell im Laufe der Zeit die Sicherheitskosten signifikant reduzieren könnte, ist die Investition in Schulungen des Personals sowie der Aufbau eines gewissenhaften Teams an Sicherheitsexperten. Genügend und kompetente Sicherheitsexperten sind genauso wichtig, wenn nicht sogar wichtiger als die Investition in neue Tools. Die besten Tools werden nicht effektiv sein, wenn sie nicht ordnungsgemäß verwaltet werden; auch dies wurde im Modell berücksichtigt.

Nach dem RAND Modell, *können Unternehmen, die sehr gewissenhaft agieren (Unternehmen mit äußerst effektiven Sicherheits- und IT-Experten im Management von Sicherheitsprogrammen) die Kosten für Cybersicherheit im ersten Jahr um 19 Prozent und im zehnten Jahr um 28 Prozent reduzieren,* im Vergleich zu Unternehmen, die weniger sorgfältig sind. .

Auch wenn es nicht genügend sachkundige Sicherheitsexperten gibt, sind die möglichen Einsparungen zu groß, als dass man sie ignorieren könnte. Unternehmen müssen sehr aggressiv vorgehen, wenn sie in Schulungen und den Ausbau ihres Sicherheitsteams investieren. Wenn keine neuen Mitarbeiter gefunden oder angenommen werden können, kann auch ein Outsourcing der spezifischen Sicherheitsfunktionen an andere Experten in Betracht gezogen werden. Der RAND Bericht zeigt, dass die Nutzung von ‚Managed Services' Vorteile bringen kann:

> *Im Kampf gegen Cyberkriminelle haben sich viele entschieden, einige wichtige Verteidigungsfunktionen an Experten auszulagern, die diese bestimmte Dienstleistung einem breiten Kundenspektrum zur Verfügung stellen. Beispielsweise führen viele Großunternehmen keine eigenen Penetrationstests ihrer Netzwerke durch, da dieses Fachgebiet so spezialisiert ist, dass es sehr schwierig ist, sachkundige Experten mit den besten Fähigkeiten zu finden und im Unternehmen zu halten.*[1]

2015

Grad der Sorgfalt	Unterschied in den Kosten von Angriffen
Sehr gering	13 % Steigerung
Gering	10 % Steigerung
Mittel	Neutral
Hoch	Neutral
Sehr hoch	6 % Verringerung

2025

Grad der Sorgfalt	Unterschied in den Kosten von Angriffen
Sehr gering	18 % Steigerung
Gering	13 % Steigerung
Mittel	Neutral
Hoch	6 % Verringerung
Sehr hoch	10 % Abnahme

[1] „The Defender's Dilemma: Charting a Course Toward Cybersecurity", RAND Corporation, 2015, Martin Libicki, Lillian Ablon und Timothy Webb.

4. Das Internet der Dinge befindet sich an einem Scheideweg

Es wird viel über IoT gesprochen und vieles davon sind übertriebene Erwartungen. Eines ist jedoch sicher: Unternehmen werden sehr bald viel mehr Geräte in ihrem Netzwerk haben als jemals zuvor. Laut RAND wird IoT einen Einfluss auf die gesamten Sicherheitskosten haben; es ist jedoch nicht klar, ob dieser positiv oder negativ sein wird. Juniper sieht Unternehmen an einem Scheideweg.

Wenn Unternehmen sich umfassend mit den sicherheitsrelevanten Folgen von IoT auseinandersetzen, und Sicherheitstechnologien sowie Gerätemanagement sinnvoll einsetzen, könnte dies langfristig zu Einsparungen führen, da die Anzahl der Geräte im Netzwerk die der herkömmlichen PCs künftig übersteigt. Andererseits könnten für Unternehmen sehr hohe Sicherheitskosten entscheiden, sollten sich IoT ähnlich entwickeln wie damals die PCs in ihren Anfangsjahren, als eine ganze Reihe an Sicherheitsproblemen gelöst werden mussten.

Im letztgenannten Szenario geht das Modell von RAND davon aus, dass die Einführung von IoT die Verluste von Unternehmen durch Cyberangriffe in 10 Jahren um 30 Prozent steigern wird.

Obwohl die meisten Unternehmen noch einige Jahre davon entfernt sind, die Auswirkungen von IoT im vollen Umfang zu erfahren, sollten sie laut Juniper schon jetzt darüber nachdenken, wie sie diese Geräte in die Sicherheitsprogramme und -netzwerke implementieren können. Unternehmen sollten sicherstellen, dass die Leistungsfähigkeit ihrer Sicherheitsinfrastruktur in der Lage ist, die erhöhte Bandbreite, die sich aus den neuen Geräten und Verbindungen ergibt, zu verwalten.

Außerdem müssen Unternehmen entscheiden, welche Sicherheitstools sie verwenden möchten, um die Einführung neuer Geräte ins Unternehmensnetzwerk zu steuern. Genau wie bei der Verwaltung von BYOD heute, müssen Unternehmen sicherstellen, dass sie die richtigen Tools haben, um neue IoT-Verbindungen schnell bereitzustellen und zu verwalten, wenn diese dem Netzwerk hinzugefügt werden. Dies heißt auch, dass eine ordnungsgemäße Rechteverwaltung implementiert und durchgesetzt werden muss, um sicherzustellen, dass diese neuen Geräte die Angriffsfläche nicht vergrößern. Zudem müssen deutliche Unternehmensrichtlinien zur Nutzung von IoT-Geräten durch Mitarbeiter am Arbeitsplatz aufgestellt und durchgesetzt werden.

5. Das Beseitigen von Software-Schwachstellen führt zu bedeutenden Kostensenkungen

Ein Bereich, der von RAND als großer Kosteneinflussfaktor identifiziert wurde, ist die Anzahl der ausnutzbaren Schwachstellen in Software und Anwendungen. Unternehmen müssen oft in Verteidigungsmaßnahmen investieren, da die grundlegenden Systeme und Software nicht sicher sind. Unglücklicherweise fällt dieser spezifische Indikator außerhalb der Kontrolle eines CISO und man muss darauf vertrauen, dass Softwarehersteller einen sichereren Code erstellen.

In dem Modell von RAND wird deutlich, dass eine Halbierung der Frequenz von Software-Schwachstellen zu einer Reduzierung der Gesamtkosten der Cybersicherheit für Unternehmen um 25 Prozent führen würde.

Allerdings ist es stark zu bezweifeln, dass Software-Schwachstellen in der Zukunft weniger häufig auftreten werden. Wenn Netzwerk- und Software-Architekturen statisch wären, würden die Verteidiger letztendlich die Oberhand gewinnen—aber Innovation macht die Informationstechnologiebranche aus.

Die Untersuchung von RAND geht davon aus, dass die Anzahl neuer Schwachstellen sehr wahrscheinlich mit der Verbreitung von Geräten durch IoT und der wachsenden Komplexität von Software-Ökosystemen, die auf Vorgängercodes beruhen, steigen wird.

Die gute Nachricht ist, dass in der Branche viel getan wird, um die Softwarequalität zu verbessern. Beispielsweise stehen Entwicklern kostenlose Tools zur Verfügung, die Schwachstellen identifizieren können, bevor Produkte geliefert werden. Wenn mehr Softwarehersteller diese Tools verwenden, wird die Anzahl der entdeckten Schwachstellen in den Produkten sehr wahrscheinlich abnehmen.

Laut Juniper obliegt es auch den Unternehmen, die Software, die sie verwenden, zu kontrollieren und bessere Sicherheitstests und Patching von den Softwareherstellern zu fordern. Wenn schlechte Sicherheit dazu führt, dass Unternehmen bestimmte Programme nicht mehr verwenden, werden Softwarehersteller einen stärkeren Anreiz haben, Produkte mit einer höheren Qualität und weniger Schwachstellen zu produzieren.

Der Weg in die Zukunft für Unternehmen und die Branche

Was können Unternehmen tun, um Sicherheitsinvestitionen im Verhältnis zu den Risiken im Zeitalter zunehmender Online-Bedrohungen besser zu verwalten?

Verwalten des Sicherheitsportfolios wie ein Geschäft

Unternehmen müssen einen Weg finden, Sicherheit wie ein Geschäft zu verwalten—also bei Entscheidungen Risiken und Vorteile quantitativ gegeneinander abzuwägen. Laut Juniper enthält das Modell von RAND mehrere umsetzbare Erkenntnisse, die Unternehmen bei der Überprüfung ihrer Sicherheitslage und -ausgaben berücksichtigen sollten.

Letztendlich sollten CISOs nach besseren Metriken suchen, um das RROI zu bestimmen. Zusammengefasst heißt dies, dass Unternehmen ihren Lebenszyklus und die Effektivität ihrer Programme kontinuierlich evaluieren müssen—genauso wie den Aktienbestand ihres Unternehmens. Hier zeigt sich die Nützlichkeit der interaktiven Modellversion von Juniper und des vollständigen Modells sowie der Methodik von RAND, da diese bei der Identifizierung der Tools hilfreich sind, die bei der Erfüllung der spezifischen Anforderungen von Unternehmen am effektivsten sind.

Evaluieren von Sicherheitstools unter Berücksichtigung von Gegenmaßnahmen

Gemäß der Erkenntnisse von RAND „können und sollten unternehmerische Entscheidungen für jegliche Investitionen die Wahrscheinlichkeit von Gegenmaßnahmen berücksichtigen, vor allem in der systembedingten Abwehr...Unternehmen sollten Maßnahmen implementieren, die wahrscheinlich keine Gegenmaßnahmen nach sich ziehen."

Juniper ist der Ansicht, dass Unternehmen sich auf die Investitionen in Tools konzentrieren sollten, die Sicherheitsaufgaben in einer zentralisierten Verwaltung und über eine ‚Distributed Enforcement Platform' automatisieren, vor allem bei der Sicherung von Netzwerken. Automation ist ein Bereich, auf den Juniper großen Augenmerk legt und es gibt verschiedene Gründe dafür, Kunden nahezulegen, in Automatisierungstools zu investieren:

- Tools mit integrierter Automation sind weniger anfällig für Gegenmaßnahmen, so dass sie im Laufe der Zeit wahrscheinlich weniger Einbußen in der Effektivität verzeichnen und ihren Wert beibehalten.
- Automation kann andere Sicherheitskosten für Unternehmen senken, indem die operationellen Anforderungen an bereits ausgelastete IT-Mitarbeiter verringert werden.
- Automation verringert die Zeit, die Sicherheitsexperten an die Konfiguration und das Testen von Systemen aufwenden, so dass sie mehr Zeit für wichtige Aufgaben haben, wie das Eindämmen von ausgefeilteren Angriffen und das Hinzufügen neuer Verteidigungsmaßnahmen.
- Außerdem kann ein zentralisiertes System dazu beitragen, Vorteile aus anderen Sicherheitsinvestitionen zu ziehen, da diese einfacher zu verwalten und auszuführen sind. Beispielsweise kann eine automatisierte und zentralisierte Verwaltung der Echtzeitdaten von Bedrohungserkennungen eine Möglichkeit bieten, das Sammelsurium an verschiedenen Quellen von Informationen zu Bedrohungen schnell zu den Durchsetzungspunkten im Netzwerk zu senden.

Weitere Informationen zu Junipers Arbeit und den Investitionen im Bereich Automation finden Sie hier.

Die Branche muss aktiv werden

Der systematische Fortschritt im Bereich Sicherheit sollte nicht allein von den CISOs getragen werden. Juniper ist der Ansicht, dass es für die gesamte Sicherheitsbranche und Regierungen unerlässlich ist, wichtige Schritte im Bereich Sicherheit zu unternehmen, um die jetzige Dynamik zu ändern und die Situation zum Vorteil der Verteidiger zu ändern.

Schulen Sie die nächste Generation

Der Schlüssel, um gegenüber den Angreifern die Oberhand zu gewinnen, liegt in der Schulung der nächsten Generation von Entwicklern, so dass diese die Innovationen, die sie schaffen, in der Zukunft besser schützen können. Der Bericht von RAND unterstützt diesen Ansatz und gibt an, dass „... sicheres Kodieren kein Bestandteil des standardmäßigen Studienplans für Computerwissenschaften ist. Diese Studenten sind die nächste Generation der Menschen, die Geräte entwickeln und entwerfen."

Wenn die nächste Generation so geschult werden kann, dass sie grundsätzlich sicherere Software erstellt, dann kann das Gefährdungspotential erheblich reduziert werden, was die Gesamtkosten der Sicherheit für Unternehmen senken würde.

Die Schulung von Studenten im Bereich Sicherheit wird auch dazu führen, dass es mehr Sicherheitsexperten geben wird und dass diese ihre Funktion effektiver ausführen werden. Indem man schon jetzt Grundlagen in diesem Bereich legt, kann die Sicherheitsbranche den momentanen Mangel an geschulten Experten vielleicht endlich überwinden. Außerdem kann die Vermittlung des Verhaltenskodex und der Ethik des Hacking dazu führen, dass zukünftige Hacker weniger geneigt sind, im Schwarzmarkt zu arbeiten, sondern ihre Fähigkeiten in anderen, positiven Bereichen einsetzen würden.

Entwicklung von Technologien unter Berücksichtigung von Gegenmaßnahmen

Auch Innovatoren im Bereich Sicherheit wie Juniper müssen weiterhin Sicherheitstechnologien schaffen, die entwickelt werden, um den Gegenmaßnahmen von Angreifern standzuhalten und die Sichtbarkeit und Kontrolle des Netzwerks zu verbessern. Obwohl das Katz-und-Maus-Spiel der Angreifer und Verteidiger endlos weitergehen wird, kann ein besser abgestimmter Ansatz zur Adressierung dieses Problems die Angreifer bei neuen Technologien länger zurückhalten.

Wir behaupten nicht, dass dieser Bericht oder das Modell die endgültige Antwort zum Verständnis von Risiken im Bereich Cybersicherheit ist. Es sollte der Anfang einer Diskussion in der Sicherheitsbranche darüber sein, wie man Risiken versteht. Wir hoffen, dass unsere Zusammenarbeit mit RAND zu einem Fortschritt führt und weitere Diskussionen anregt.

Der vollständige Bericht der RAND Corporation sowie der Bericht des letzten Jahres und weitere Materialien von Juniper, finden Sie hier.

Über diesen Bericht

„The Defender's Dilemma: Charting a Course Toward Cybersecurity", RAND Corporation, 2015, Martin Libicki, Lillian Ablon und Timothy Webb. Basierend auf Tiefeninterviews, die zwischen Oktober 2013 und August 2014 mit CISOs über deren aktuelle und zukünftige Bedrohungslage geführt wurden. Diese Untersuchung basiert auf dem ersten Bericht einer von Juniper gesponserten zweiteiligen Serie von RAND, „Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar," der die wirtschaftlichen Triebfedern für Angreifer und den ausgefeilten Schwarzmarkt untersucht, den sie zur Verstärkung ihrer Bemühungen aufgebaut haben.

Unternehmens- und Vertriebshauptsitz

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Telefon: 888.JUNIPER (888 586 4737)
oder +1 408 745 2000
Fax: +1 408 745 2100
www.juniper.net

APAC und EMEA Hauptsitze

Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, Niederlande
Telefon: +31 0 207 125 700
Fax: +31 0 207 125 701

JUNIPER NETWORKS

Juniper Networks (NYSE: JNPR) bietet Innovationen in den Bereichen Routing, Switching und Sicherheit. Innovationen in Software, Silizium und Systemen durch Juniper Networks verändern die Qualität und die Wirtschaftlichkeit des Netzwerks. Weitere Informationen finden Sie bei Juniper Networks (www.juniper.net) oder wenn Sie sich mit Juniper auf Twitter oder Facebook verbinden.