

Zusammenfassung

Cisco Annual Security Report 2015

Die Bedrohungslandschaft bleibt auch weiterhin hochdynamisch.

Cyberkriminelle verfeinern laufend ihre Angriffsmethoden und entwickeln immer neue Techniken, um unerkannt in Systeme einzudringen und ihre Aktivitäten zu verschleiern. Sicherheitsteams in Unternehmen müssen daher permanent ihre Maßnahmen anpassen, um Firma und Benutzer vor immer raffinierteren Angriffen zu schützen.

Die Benutzer spielen eine zentrale Rolle. Sie sind nicht nur die Ziele der Angreifer, sondern spielen ihnen häufig auch unbewusst in die Hände.

Die Cisco Sicherheitsexperten analysieren im *Cisco Annual Security Report 2015* die aktuellen Entwicklungen im Bereich der IT-Sicherheit. Neben der Rolle von Angreifern und Verteidigern liegt dabei ein besonderes Augenmerk auf den Benutzern, denn diese geraten zunehmend zum schwächsten Glied in der Sicherheitskette eines Unternehmens.

Das Thema Cybersicherheit ist äußerst breit gefasst und komplex und hat auf Privatanutzer ebenso große Auswirkungen wie auf Unternehmen, Regierungen und andere Einrichtungen weltweit. Der *Cisco Annual Security Report 2015* ist in vier Themenkomplexe gegliedert. Auf den ersten Blick kann der Eindruck entstehen, die darin behandelten Probleme stünden nur für sich allein. Bei genauerer Betrachtung wird jedoch deutlich, wie stark sie einander beeinflussen und miteinander in Zusammenhang stehen:

Die vier Themenkomplexe des *Cisco Annual Security Report 2015*:

1. Entwicklungen im Bedrohungsumfeld
2. Ergebnisse der *Security Capabilities Benchmark Study*
3. Geopolitische und Branchentrends
4. Cybersicherheit neu überdenken – vom Benutzer bis in die Führungsetage

Laden Sie den Cisco Annual Security Report 2015 hier herunter:
www.cisco.com/go/asr2015



1. Entwicklungen im Bedrohungsumfeld

Dieser Abschnitt bietet einen Überblick über aktuelle Ergebnisse aus der Bedrohungsforschung von Cisco sowie die neuesten Trends bei Exploit-Kits, Spam, Bedrohungen, Sicherheitslücken und Malvertising (böartige Online-Werbung). Beleuchtet werden außerdem die zunehmend von Cyberkriminellen eingesetzten Methoden, die Aktivitäten der Benutzer als Ausgangspunkt für ihre Angriffe zu nutzen. Die Grundlage für die Ermittlung der Trends im Jahr 2014 bildet ein umfangreicher Satz an globalen Telemetriedaten, die von den Experten von Cisco Security Research analysiert wurden.

2. Ergebnisse der Security Capabilities Benchmark Study

Cisco hat in neun Ländern Chief Information Security Officer (CISO) und Sicherheitsteams aus Unternehmen unterschiedlicher Größe zu ihren Sicherheitsressourcen und -verfahren befragt, um zu ermitteln, wie diese den aktuellen Sicherheitsstatus ihres Unternehmens einschätzen. Die Ergebnisse der Studie finden Sie exklusiv im *Cisco Annual Security Report 2015*.

3. Geopolitische und Branchentrends

In diesem Abschnitt gehen Experten von Cisco für Sicherheit, Geopolitik und Richtlinien auf aktuelle geopolitische Trends ein, die Unternehmen insbesondere multinationale Konzerne – im Auge behalten sollten. Zentrales Thema dabei: Die Zunahme der Cyberkriminalität in Regionen mit schwachen staatlichen Strukturen. Ebenfalls diskutiert werden aktuelle globale Entwicklungen in den Bereichen Datensouveränität, Datenlokalisierung, Verschlüsselung und Datenkompatibilität.

4. Cybersicherheit neu überdenken – vom Benutzer bis in die Führungsetage

Um Sicherheit heute effektiv gewährleisten zu können, müssen Unternehmen das Thema Cybersicherheit neu überdenken. Die Experten von Cisco betonen: Sowohl vor als auch während und nach einem Angriff müssen fortschrittliche Sicherheitskontrollen implementiert werden. Ein wichtiger Appell lautet außerdem: Sicherheit muss Chefsache werden. Wollen Unternehmen ihren Angreifern einen Schritt voraus sein, müssen sie darüber hinaus anpassungsfähiger werden. Möglich wird dies durch einen Sicherheitsansatz, der auf den Prinzipien des „Cisco Sicherheitsmanifest“ basiert.

Die im *Cisco Annual Security Report 2015* behandelten Themen laufen in der Gesamtschau auf Folgendes hinaus: Die Angreifer verstehen um ihre schädlichen Aktivitäten zu verbergen. Benutzer und Sicherheitsteams sind gleichermaßen Teil des Problems. Viele Sicherheitsverantwortliche halten ihre Sicherheitsprozesse und -tools zwar für effektiv, tatsächlich besteht jedoch häufig Nachholbedarf. Geopolitische Entwicklungen – von der Gesetzgebung verschiedener Länder bis hin zur Sicherheitslage in bestimmten Regionen – müssen genau beobachtet werden. Denn diese können direkte Auswirkungen auf den Geschäftsbetrieb von Unternehmen sowie darauf haben, wie sie das Thema Sicherheit angehen. Alle diese Faktoren machen deutlich: Unternehmen aller Größenordnungen müssen erkennen, dass es bei der Sicherheit auf die Benutzer ankommt, dass Kompromittierungen unvermeidlich sind und dass es genau jetzt an der Zeit ist, ihren Sicherheitsansatz auf den Prüfstand zu stellen.



Hauptgeschäftsstelle Nord- und Südamerika
Cisco Systems, Inc.
San Jose, CA

Hauptgeschäftsstelle Asien-Pazifik-Raum
Cisco Systems (USA) Pte. Ltd.
Singapur

Hauptgeschäftsstelle Europa
Cisco Systems International BV
Amsterdam, Niederlande

Cisco verfügt über mehr als 200 Niederlassungen weltweit. Die Adressen mit Telefon- und Faxnummern finden Sie auf der Cisco Website unter www.cisco.com/go/offices.

Cisco und das Cisco Logo sind Marken oder eingetragene Marken von Cisco und/oder Partnerunternehmen in den Vereinigten Staaten und anderen Ländern. Eine Liste der Cisco Marken finden Sie unter www.cisco.com/go/trademarks. Die genannten Marken anderer Anbieter sind Eigentum der jeweiligen Inhaber. Die Verwendung des Begriffs „Partner“ impliziert keine gesellschaftsrechtliche Beziehung zwischen Cisco und anderen Unternehmen. (1110R)