Medienkontakt:
Susanne Sothmann / Erna Kornelis
Kafka Kommunikation
089 74 74 70 580
ssothmann@kafka-kommunikation.de
ekornelis@kafka-kommunikation.de

Neueste IDG-Studie: Cyber Defense Maturity Report 2014

Mangelndes Vertrauen in die IT-Sicherheit durch inkonsequente Investitionen, Trends bei Sicherheitsvorfällen und -kontrollen, verbesserungswürdige Bereiche in 1600 IT-Unternehmen.

CAMPBELL, Kalifornien, 15. Juli 2014 — ForeScout Technologies, Inc., führender Anbieter von Lösungen für intelligente Zugangskontrolle und Security Management, veröffentlicht heute seine neueste Studie, den Cyber Defense Maturity Report 2014. Die unabhängige Studie von IDG Connect steht hier zum Download zur Verfügung und liefert neueste Erkenntnisse:

- zur Art der Sicherheitsereignisse in Unternehmen
- zur wahrgenommenen Ausgereiftheit der Prozesse, Kontrollen und Tools, die zur Vorbeugung und Entschärfung von Anfälligkeiten eingesetzt werden
- zum Grad des Vertrauens auf die Wirksamkeit der Sicherheitsmaßnahmen zu denjenigen Bereichen, in denen künftige Investitionen und Verbesserungen am wahrscheinlichsten sind.

Für die Studie wurden im Mai und Juni 2014 1600 Entscheidungsträger der IT-Sicherheit befragt, die in Unternehmen mit mehr als 500 Mitarbeitern in den USA, Großbritannien, Deutschland, Österreich und der Schweiz, aus den Sektoren Finanzwesen, Produktion, Gesundheitswesen, Einzelhandel und Bildungswesen, tätig sind.

Zu den zentralen Ergebnissen der Studie zählt, dass sich im vergangenen Jahr in mehr als 96 Prozent der Unternehmen ein bedeutender IT-Sicherheitsvorfall ereignete. Die Mehrzahl der befragten IT-Unternehmen sind sich bewusst, dass ein Teil ihrer Sicherheitsmaßnahmen unausgereift oder ineffektiv sind, doch nur 33 Prozent sind sehr zuversichtlich, dass sie die weniger ausgereiften Sicherheitskontrollen verbessern können. Zudem machen die Ergebnisse deutlich, dass die wachsenden betrieblichen Komplexitäten und Bedrohungen die Sicherheitskapazitäten beeinträchtigt haben: Mehr als 43 Prozent der Befragten halten die Verhinderung, Identifizierung, Diagnose und Behebung von Problemen heute für schwieriger als

noch vor zwei Jahren. In einem von sechs Unternehmen kam es in den letzten zwölf Monaten zu fünf oder mehr bedeutenden Sicherheitsereignissen. Während die Befragten das IT-Sicherheitsmanagement offenbar mit Zuversicht betrachten, tut sich bei den Ergebnissen in denjenigen Bereichen, in denen die Vorfälle die größten Auswirkungen hatten, ein Widerspruch auf zwischen der Effizienz der Maßnahmen und den voraussichtlichen Investitionen in selbige.

Highlights der Ergebnisse

Der vollständige Cyber Defense Maturity Report 2014 enthält ausführliche Daten, Analysen und Rückschlüsse. Hier einige Highlights:

- In jedem sechsten Unternehmen ereigneten sich fünf oder mehr bedeutende Sicherheitsvorfälle; in 39 Prozent der Unternehmen waren es zwei oder mehr Vorfälle.
- Die häufigsten Sicherheitsvorfälle waren Phishing, Verletzung von Compliance-Richtlinien, Verwendung nicht genehmigter Geräte und Anwendungen sowie unbefugte Datenzugriffe.
- 40 Prozent der Befragten erklärten, die Aufgaben des Sicherheitsmanagements seien heute schwieriger als vor zwei Jahren; insbesondere die Verhinderung, Diagnose, Identifizierung und Behebung von Problemen.
- Am häufigsten genannt wurden Sicherheitsprobleme in folgenden Bereichen: Malware und hochentwickelte Bedrohungen, Anwendungs- und Wireless-Sicherheit, Zugriff auf Netzwerkressourcen, Verwendung nicht genehmigter Anwendungen und persönlicher Mobilgeräte sowie Datenlecks.
- Relativ unausgereift sind nach Ansicht der Befragten die Kontrollmaßnahmen in folgenden Bereichen: Verwendung persönlicher Mobilgeräte, Perimeter-Bedrohungen, Inventarmanagement und Endpunkt-Compliance, Sicherheitsprobleme im Zusammenhang mit Virtualisierung, Schadgeräte sowie Anwendungssicherheit. Dennoch bekundeten nur 54 Prozent der Befragten ein gewisses Maß an Zuversicht, dass sich die Situation in den nächsten 12 Monaten verbessern werde.
- Mehr als 61 Prozent bekundeten wenig bis gar keine Zuversicht hinsichtlich folgender Bereiche: Ein- und Übersicht bei Netzwerkgeräten, Einhaltung von Konfigurationsstandards und Abwehrmaßnahmen bei Geräten sowie Richtlinienkonformität von virtuellen Maschinen und Remote-Geräten.

- Die fünf Sicherheitstechnologien, die nach Ansicht der Befragten den größten Interoperabilitätswert haben, sind Firewalls, Malwareschutz, Netzwerk-Zugangskontrolle (NAC), Mobilgeräte-Management (MDM) und hochentwickelte Bedrohungserkennung (Advanced Threat Detection, ATD).

Branchenbezogene und regionale Highlights

- Malware- und APT-Angriffe wurden in sämtlichen Branchen und Regionen als Top-Priorität eingestuft, doch scheint die Wahrscheinlichkeit geringer, dass weitere Ressourcen in die Verminderung von Perimeter-Angriffen investiert werden.
- Zusammengefasst kam es bei den Befragten in allen drei Regionen in den letzten 12 Monaten durchschnittlich 2,6 Mal zu erheblichen Verletzungen von Compliance-Richtlinien, deren Aufarbeitung viel Zeit in Anspruch nahm. In den USA lag die Zahl jedoch höher als im UK und in den DACH-Ländern.
- Die Sektoren Produktion, Bildung und Finanzen sind offenbar anfälliger für Phishing-Angriffe, während im Gesundheitsbereich eher überdurchschnittlich viele Verletzungen der Compliance-Richtlinien zu beobachten waren. Eine Ausnahme bildet jedoch der Gesundheitssektor in Deutschland: Hier ereigneten sich mehr Zwischenfälle im Zusammenhang mit der Verwendung nicht genehmigter Anwendungen und Geräte sowie Systemkompromittierungen.
- Die Befragten aus dem Gesundheitswesen äußerten mehr Bedenken im Hinblick auf das Monitoring von Datenlecks als die Befragten aus den Bereichen Produktion, Bildung, Einzelhandel und Finanzen; insbesondere in der DACH-Region, wo die nicht genehmigte Verwendung von Geräten und Anwendungen sowie Systemkompromittierungen problematischer scheinen.
- Finanzinstitute waren von mehr Zwischenfällen betroffen, die durch Phishing-Angriffe, Verletzung von Compliance-Richtlinien, nicht genehmigte Verwendung von Anwendungen sowie Datenlecks verursacht wurden. Außerdem empfanden die Finanzinstitute die Behebung von Problemen im Vergleich zu anderen Sektoren insgesamt als schwieriger. Besonders für die DACH-Region gilt, dass im Finanzsektor die Wireless-Sicherheit ein weiteres großes Problem ist.
- Die Definition von Richtlinien, die technischen Kontrollen und die Korrektur-Kapazitäten sind im Bildungssektor offenbar am wenigsten ausgereift, während sie im Finanzsektor im

Allgemeinen am ausgereiftesten erscheinen. In der DACH-Region scheinen diese Bereiche allerdings im Produktionswesen am besten entwickelt zu sein.

- In den Ländern der DACH-Region herrscht im Hinblick auf Verbesserungen bei Inventarmanagement-Tools weniger Zuversicht als im UK und den USA.
- Im Durchschnitt erklärten 78 Prozent aller Befragten, dass BYOD Auswirkungen auf Governance, Risk & Compliance (GRC) habe. Während der Einzelhandelssektor im Hinblick auf die BYOD-Sicherheit fortschrittlicher zu sein scheint, waren die europäischen Teilnehmer generell der Ansicht, dass sich Datenlöschung und Verschlüsselung stärker auf GRC auswirken.

„Die Erkenntnisse des von IDG Connect durchgeführten Cyber Defense Maturity Report 2014 bieten eine aufschlussreiche Momentaufnahme der derzeitigen Anfälligkeiten, Kontrollmaßnahmen und Investitionen in einer Reihe von Regionen und Branchen“, erklärt Scott Gordon, Chief Marketing Officer bei ForeScout. „Diese unabhängige Untersuchung zeigt deutlich, wie notwendig Fähigkeiten für kontinuierliches Monitoring, Ein- und Übersicht sowie Problembehebung sind – Fähigkeiten, die Lösungen für intelligente Zugangskontrolle und Security Management, von ForeScout beispielhaft in sich vereinen.“

Die vollständige Studie und die Infografik stehen auf www.forescout.com/stateofdefense zum Download bereit. Weitere Vergleiche nach Regionen und Branchen werden ebenfalls zur Verfügung gestellt. Am 31. Juli um 17:00 Uhr veranstalten IDG Connect und ForeScout auf www.forescout.com/sodwebcast einen Live-Webcast mit dem Titel „IT Cyber Defense – Progress and Denial“, in dem sie die Erkenntnisse der Studie präsentieren.

Über ForeScout

ForeScout ist der führende Anbieter für intelligente Zugangskontrolle und Security Management und bietet Unternehmen umfassende Sichtbarkeit, Transparenz und richtlinienbasierte Kontrolle über Nutzer, Geräte und Anwendungen im Netzwerk. Dies erlaubt es Unternehmen, ihr Netz kontinuierlich zu monitoren und Sicherheitsvorfälle sowie Cyberattacken automatisch zu beheben. ForeScouts CounterACT ist leicht zu implementieren, offen und skalierbar und wird bereits von über 1500 Unternehmen und Regierungsorganisationen eingesetzt. ForeScout hat

seinen Hauptsitz in Campbell, Kalifornien, und vertreibt seine Lösungen über ein Netzwerk von autorisierten Partnern weltweit. Weitere Informationen finden Sie unter www.forescout.com