IBM X-Force 2011 Trend- und Risikobericht zur Jahreshälfte 2011

Prioritäten der CIOs beim Thema Sicherheit

„Die Welt von heute ist vernetzter, intelligenter und instrumentierter: So sehr diese Innovationen unsere Effizienz und unsere Fähigkeit verbessern, innerhalb kürzester Zeit weltweite Verbindungen herzustellen, so sehr können die damit verbundenen Risiken und Gefahren zunehmen und sich nur schwer kontrollieren lassen.“

— IBM X-Force Research & Development

In der ersten Jahreshälfte 2011 war ein geradezu explosionsartiger Anstieg bei den Sicherheitsverstößen festzustellen. Nahezu täglich treffen neue Berichte ein. Aus diesem Grund wurde das Jahr 2011 zum „Jahr der Sicherheitsverletzungen“ erklärt. Kennzeichnend für die Sicherheitsverletzungen ist nicht nur deren Häufigkeit, sondern auch die Tatsache, dass sich die Angriffe zunehmend gegen führende Mitarbeiter eines Unternehmens richten, die Zugriff auf wichtige Daten haben. Das Umfeld verändert sich: Die Grenzen der Geschäftsinfrastruktur dehnen sich immer weiter aus und verwischen in einigen Fällen. Herbeigeführt wird diese Entwicklung durch Faktoren wie Cloud-Computing, Mobilität, Social Business, Big Data und vieles mehr. Zudem werden die Attacken immer ausgereifter. Kennzeichnend dafür ist die mit hoher Sorgfalt und Akribie ausgeführte Planung, bei der bereits langfristig wichtige Daten gesammelt werden, um einen Angriff möglichst gezielt ausführen zu können. Die Auswirkungen solcher Angriffe sind mittlerweile so gravierend, dass sie nicht mehr ausschließlich den technischen Bereich beschäftigen, sondern auch in den Führungsetagen für Gesprächsstoff sorgen.

Die kritischsten Bereiche sind nachfolgend aufgeführt:

- Die gebräuchlichsten Angriffsmethoden sind SQL-Injection und Brute-Forcing-Attacken gegen Kennwörter, Datenbanken und gemeinsam genutzte Microsoft® Windows®-Ordner/-Laufwerke. Dabei durchsuchen die Hacker das Internet nach offenen Services und versuchen, in diese einzudringen.
- Die Anzahl der kritischen Schwachstellen liegt bereits über allen im Jahr 2010 gemeldeten Vorfällen, wobei es sich bei nahezu allen Schwachstellen um Probleme im Bereich der Remote-Codeausführung handelt, die sich auf wichtige Softwareprodukte in den Unternehmen auswirken.
- Deutlicher Anstieg bei den Sicherheitsproblemen bei Dokumentlesern und Multimedia-Playern. Die Angreifer konzentrieren sich dabei auf Software, die Benutzer unabhängig vom bevorzugten Browser ausführen – in diesem Bereich ist daher die Anzahl der betroffenen Benutzer pro Exploit am größten.
- 40 Prozent von 678 Fortune 500-Websites und anderen häufig genutzten Websites weisen clientseitige Java™ Script-Schwachstellen auf.

Der X-Force Threat Analysis-Service ist ein Service, der täglich angepasst wird. Er informiert Ihre IT-Mitarbeiter über aktuelle Bedrohungen, verfügbare Schutzmechanismen und allgemeine Trends in der Branche, damit sich Ihr Unternehmen proaktiv auf die wachsenden Gefahren vorbereiten können.

Paradoxerweise wurden in diesem Jahr bereits viele Anstrengungen für mehr Sicherheit im Internet unternommen, durch die zahlreiche Statistiken zu Schwachstellen und Angriffen deutlich verbessert werden konnten.

- Im Jahr 2011 ist festzustellen, dass das Spam-Volumen weiter zurückgeht, was letztendlich auch darauf zurückzuführen war, dass das Rustock-Botnet außer Gefecht gesetzt werden konnte.
- In der ersten Jahreshälfte 2011 haben sich die Spammer scheinbar vom traditionellen E-Mail-Phishing verabschiedet. Der Prozentsatz der Spam, die im Wochenrhythmus ihre Phishingattacken ausführt, liegt im Wochenschnitt unter 0,01 Prozent.
- In den vergangenen Jahren waren ca. die Hälfte der festgestellten Sicherheitsverletzungen Verstöße bei Webanwendungen. Dieser Wert ist in diesem Jahr auf 37 Prozent zurückgegangen, wobei besonders bei der Anzahl der SQL-Injection-Vorfälle ein deutlicher Rückgang festzustellen war.
- Außerdem geht die Anzahl der hoch kritischen und kritischen Sicherheitsverstöße im Browserumfeld kontinuierlich zurück, obwohl der Browsermarkt deutlich diversifizierter und umkämpfter geworden ist.

Auch wenn in zentralen Bereichen einige Erfolge erzielt werden konnten, ist der Kampf beileibe noch nicht zu Ende. Die Angreifer haben nämlich ihre Aktivitäten in neue Bereiche verlagert, so z. B. auf das Smartphone. Die schnelle Verbreitung dieser Geräte hat in Kombination mit der Konsolidierung bei den Betriebssystemen dazu geführt, dass die Angreifer bereits in den Startlöchern stehen, um die Chancen zu nutzen, die diese Geräte bieten. Aus Sicht der IBM X-Force Research and Development-Teams geht man davon aus, dass sich die Anzahl der Sicherheitsverletzungen bei den Betriebssystemen für mobile Geräte im Vergleich zum Jahr 2010 mehr als verdoppeln wird.

Wie können Sie sich dagegen wehren? Wäre das IBM X-Force Research and Development-Team in dieser neuen, deutlich komplexeren Umgebung mit dem Management Ihres Netzwerks befasst, würden wir wie folgt vorgehen:

1. Durchführung regelmäßiger externer und interner Sicherheitsprüfungen von Drittanbieterprodukten
2. Überwachung der Endgeräte
3. Segmentierung vertraulicher Systeme und Informationen
4. Schutz des Unternehmensnetzwerks
5. Prüfung der Webanwendungen
6. Schulung von Endbenutzern zu Themen wie Phishing und Spear Phishing
7. Suche nach unsicheren Kennwörtern
8. Berücksichtigung von Sicherheitsthemen in jedem Projektplan
9. Überprüfung der Richtlinien der Geschäftspartner
10. Ausarbeitung eines ausführlichen Notfallplans bei Störfällen

Weitere Informationen finden Sie im Gesamtbericht.

Das IBM X-Force Research and Development-Team hat festgestellt, dass die wahrscheinlichste Ursache für das Verschwinden des SQL Slammer ein White (oder Black) Knight war. Lesen Sie mehr dazu im Gesamtbericht.

Informationen zu IBM X-Force Research and Development und zur Zusammenarbeit mit dem Bereich IBM Security

IBM Security steht für verschiedene Brands, die ein breites Spektrum zum Thema Sicherheitskompetenz abdecken.

- Während sich die IBM X-Force Research and Development-Teams mit der Analyse aktueller Trends und Methoden von Angreifern befassen, nutzen andere Gruppen innerhalb von IBM diese aussagekräftigen Daten für die Entwicklung von Schutzmechanismen für unsere Kunden.
- Die X-Force Research and Development-Teams sind in der Lage, die unterschiedlichsten Bedrohungen und Schwachstellen bei der IT-Sicherheit zu erkennen, analysieren, überwachen und erfassen.
- Der Bereich IBM Managed Security Services (MSS) ist für die Überwachung von Exploits in Bezug auf Endgeräte, Server (einschließlich Web-Server) und die allgemeine Netzwerkinfrastruktur zuständig.
- Die MSS-Mitarbeiter verfolgen über das Web sowie andere Quellen wie E-Mail und Instant Messaging verbreitete Exploits.
- IBM Professional Security Services (PSS) bietet Services wie umfassende, unternehmensweite Sicherheitsbewertung, Design- und Implementierungsservices für den Aufbau effizienter IT-Sicherheitslösungen.
- Unser Content Security-Team durchsucht und kategorisiert das Web in Form von Crawlersuchen, unabhängigen Erkennungsmechanismen und mithilfe der von MSS bereitgestellten Informationen.
- IBM hat praxisorientierte Daten zu Schwachstellen und Sicherheitslücken im Rahmen von Sicherheitstests zusammengetragen, die in den vergangenen Jahren vom IBM Rational Services-Team durchgeführt wurden. Diese Daten spiegeln eine Kombination aus Analyseergebnissen zur Anwendungssicherheit von IBM Rational AppScan und manuellen Sicherheitstests und -prüfungen wider. Von den Anforderungen, über Design, Code und Produktion ermöglicht IBM Rational AppScan ein umfassendes Management von Anwendungsschwachstellen im gesamten Anwendungslebenszyklus.
- Mit den IBM Cloud Security Services kann der Kunde Sicherheitssoftware über ein gehostetes Lizenzierungsmodell nutzen, das nicht nur hilft, Kosten zu senken, sondern auch die Servicebereitstellung und die Sicherheit verbessert.
- Lösungen für das Identitäts- und Zugriffsmanagement ermöglichen ein effizientes Identitäts- und Zugriffsmanagement sowie benutzerspezifische Compliancеprüfungen. Mit diesen Lösungen lassen sich alle Managementabläufe in Bezug auf Benutzer, Authentifizierung, Zugriffe, Prüfrichtlinien und die Bereitstellung von Benutzerservices zentralisieren und automatisieren.
- IBM Lösungen zur Daten- und Informationssicherheit bieten alle notwendigen Funktionen für einen ausreichenden Datenschutz und ein effizientes Zugriffsmanagement, wodurch die unternehmensweite Sicherheit im gesamten Lebenszyklus von Informationen sichergestellt ist.

Weitere Informationen

Weitere Informationen zum X-Force Trend- und Risikobericht für 2011 finden Sie unter: **ibm.com**/security

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustrasse 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

Dieses Dokument ist eine Kurzübersicht zu dem von IBM veröffentlichten Gesamtbericht „IBM X-Force 2011 Mid-year Trend and Risk Report“. Der vollständige Bericht kann über die folgende Adresse abgerufen werden: **ibm.com**/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=SWGE_WG_WG_USEN&htmlfid=WGL03009USEN&attachment=WGL03009USEN.PDF

Bitte der Wiederverwertung zuführen

WGE03015-DEDE-00