Hewlett Packard Enterprise

CYBER RISK Report 2016

Der jährlich erscheinende Cyber Risk Report von HP Security Research vermittelt Unternehmen einen Überblick über vorhandene Gefahren und stellt Informationen zur Minimierung von Sicherheitsrisiken bereit. Der diesjährigen Bericht zeigt Perspektiven auf, die sich aus den Möglichkeiten erweiterter Datenanalyse ergeben. Außerdem werden verschiedene Technologien wie Open Source, Mobiltechnologie und das Internet der Dinge genauer unter die Lupe genommen.

35%

Mehr als ein Drittel der überprüften Anwendungen (35 Prozent) wiesen mindestens eine kritische oder schwerwiegende Schwachstelle auf.

Fast **86%** der befragten Unternehmen verwenden IDS.

Die Verwendung von Open Source-Komponenten in Anwendungen greift immer mehr um sich. **14%**

153%

Über 10.000 neue Bedrohungen werden täglich auf der Android-Plattform erkannt. Dies entspricht einer Steigerung gegenüber dem Vorjahr von 153 %.

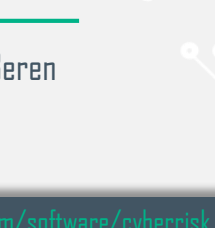
80%

Mehr als 80 % der Open Source- und kommerziellen Anwendungen weisen Schwachstellen bei Sicherheitsfunktionen auf, was schwerwiegende Folgen für das Management persönlicher Daten hat.

95 % der neu entdeckten Malware und 42 % der Angriffe auf Schwachstellen zielen auf Windows. Das Betriebssystem bleibt damit das vorherrschende Angriffsziel.

Mobile Anwendungen mit Datenlecks im internen System verdeutlichen die Bedenken beim Speichern geschäftskritischer Daten auf Geräten, die leicht verloren gehen können.

29 % aller ausgenutzten Schwachstellen, die 2015 entdeckt wurden, haben weiterhin einen 2010 Stuxnet-Infektionsvektor verwendet, der bereits zweimal gepatcht wurde.



Das Jahr des Kollateralschadens

Datensicherheitsverletzungen sind schon längst nicht mehr auf den Diebstahl von Zahlungskartendaten beschränkt. Vielmehr holen sich Angreifer Informationen, die das Leben einer Person nachhaltig ändern können.

Zu strikte Vorschriften drängen Forschung in den Untergrund

Diverse vorgeschlagene Vorschriften zum Thema Cybersicherheit hätten zur Folge, dass legitime Sicherheitsforschungen in den Untergrund gedrängt werden. Diese Vorschriften sollten jedoch Forschung schützen und fördern, die auf die allgemeine Sicherheit zielt.

Umstieg von Einzellösungen auf Komplettlösungen

2015 sind viele Anbieter dazu übergegangen, Schutzmechanismen zu entwickeln, die eine ganze Angriffsklasse unterbinden.

Politischer Druck zielt auf Trennung von Datenschutz- und Sicherheitsbestrebungen

Viele Gesetzgeber in den USA, Großbritannien und anderen Ländern vertreten die Ansicht, dass Sicherheit nur durch eine Einschränkung der Grundrechte von Datenschutz und ordentlichen Gerichtsverfahren gewährleistet werden kann.

Branche macht keinerlei Fortschritt in puncto Patching im Jahr 2015

Die im Jahr 2015 am meisten ausgenutzte Schwachstelle ist bereits mehr als fünf Jahre alt, wurde bereits 2014 am meisten ausgenutzt und zweimal vom Anbieter gepatcht.

Angreifer richten Angriffe direkt auf Anwendungen

Anwendungen gelten derzeit als einfachster Punkt, über den Angreifer auf sensitive Unternehmensdaten zugreifen.

Die Monetarisierung von Malware

ATM-Malware wird immer beliebter und verhilft Cyberkriminellen schneller zu größeren Gewinnen.

Den gesamten Bericht finden Sie unter www.hpe.com/software/cyberrisk