IDC INFOBRIEF ZUSAMMENFASSUNG

Wirtschaftliche Auswirkungen von Malwareinfektionen aufgrund der Nutzung raubkopierter Software: Häufig gestellte Fragen

November 2017
Gesponsert von Microsoft

F: Worum geht es in dieser Studie?

A: Diese Studie zeigt auf, dass bei der Nutzung raubkopierter Software die latente Gefahr besteht, sein System mit einer Malware zu verseuchen, was zu gravierenden Sicherheitsproblemen führen kann. Darüber hinaus informiert diese Studie über die Kosten, die im Privatbereich und in Unternehmen anfallen können, um von Malware verursachte Sicherheitsprobleme zu beheben. Zudem geht sie darauf ein, welche Verhaltensweisen zu Sicherheitsproblemen führen können. Dabei geht es ausschließlich um raubkopierte PC-Software. Server-Anwendungen und Apps für Smartphones spielen in dieser Studie keine Rollen.

F: Warum wurde diese Studie durchgeführt?

A: Diese Studie soll Privatanwendern und Unternehmen die Gefahren, die die Nutzung raubkopierter Software mit sich bringen, vor Augen führen. Denn der vermeintliche „Vorteil", der sich aus der Nutzung raubkopierter Software ergibt, steht in keinem Verhältnis zu den damit verbundenen Risiken.

F: Von wem wurde diese Studie durchgeführt?

A: Diese Studie wurde von IDC (International Data Corporation) durchgeführt. Das weltweit tätige Marktforschungs- und Consultingunternehmen beschäftigt über 1.000 Analysten und verfügt über Zweigstellen in mehr als 50 Ländern. IDC ist unter anderen auch für die zweijährliche, von der Business Software Alliance (BSA) in Auftrag gegebene Studie zum Thema unlizenzierte Software verantwortlich. Bisher hat IDC sieben solcher Studien veröffentlicht. Die erste Studie wurde im Auftrag von Microsoft 2006 durchgeführt und 2007 veröffentlicht.

F: Wie wird raubkopierte Software definiert?

A: Im Rahmen dieser Studie beschreibt der Ausdruck raubkopierte Software sowohl Software, die gefälscht oder anderweitig manipuliert wurde, als auch Original-Software, die ohne Bezahlung – also unlizenziert – verwendet wird. Im Zusammenhang mit den finanziellen Folgen, die durch Malware verursacht werden, bezieht sich der Ausdruck raubkopierte Software hingegen ausschließlich auf gefälschte oder manipulierte Software, da davon ausgegangen wird,

dass Original-Software nicht mit Malware verseucht ist.

F: Die Studie zeigt eine Korrelation zwischen der Nutzung raubkopierter Software und dem Auftreten von Malware. Doch eine Korrelation ist noch lange keine Kausalität, oder?

A: Das stimmt. Allerdings weisen die Daten, die wir im Rahmen dieser Studie gesammelt haben, ganz klar auf eine Kausalität zwischen raubkopierter Software und Malware hin. Zudem belegen die Forschungsergebnisse anderer Unternehmen, dass raubkopierte Software für Personen, die Malware entwickeln und in Umlauf bringen, eine große Rolle spielt. Ein im Mai 2017 in der New York Times veröffentlichter Artikel, in dem es um die Nutzung raubkopierter Software in China geht, verdeutlicht diesen Zusammenhang: https://www.nytimes.com/2017/05/15/business/china-ransomware-wannacry-hacking.html?mcubz=0&_r=0.

F: Wie wird die Anzahl der Infektionen, die sich aufgrund der Nutzung raubkopierter Software ergeben, berechnet?

A: IDC verfügt über eine interne Datenbank, in der alle Informationen gespeichert sind, die im Zusammenhang mit der zweijährlichen, im Auftrag der BSA durchgeführten Studie gewonnen werden. Dadurch sind wir in der Lage, die Häufigkeit von Malwareinfektionen basierend auf der Quelle der raubkopierten Software anzugeben, zum Beispiel auf dem PC vorinstallierte Programme oder aus dem Web geladene Software. Dieser Infektionsfaktor wurde in dieser Studie auf alle Arten von raubkopierter Software angewandt.

F: Viele Malwareinfektionen lassen sich beheben, oder?

A: So ist es. Und die Tatsache, dass Privatanwender und Unternehmen Malware in Quarantäne stellen oder löschen können, haben wir bei den finanziellen Auswirkungen selbstverständlich berücksichtigt. Ein Faktor, der hierbei eine große Rolle spielt, ist die Häufigkeit, mit der Softwaresicherheitsupdates installiert werden.

F: Die finanziellen Auswirkungen für Privatanwender und Unternehmen summieren sich allein in Europa auf über 58 Milliarden Euro. Das ist ein extrem hoher Betrag.

A: Ja, das ist viel Geld. Im Vergleich zu anderen Beträgen relativiert sich die Höhe allerdings: So werden in diesem Jahr allein in Europa mehr als 130 Milliarden Euro in neue PC-Hardware investiert, die Gesamtinvestitionen in die IT übersteigen 500 Milliarden Euro, und die Summe der Erlöse aller Unternehmen beträgt mehr als 50 Billionen Euro. Nahezu die Hälfte der Investitionen von Unternehmen steht übrigens im Zusammenhang mit der Behebung von Datenpannen.

F: Warum spielen im Zusammenhang mit Privatanwendern die Kosten eine Rolle? Die Zeit, die sie in die Entfernung von Malware investieren, wird doch nicht bezahlt.

A: Das stimmt. Allerdings gibt es bei der Quantifizierung des Aufwands, den Privatanwender betreiben müssen, um Malware zu entfernen, keine andere Möglichkeit, als die aufgewendete Zeit in „Kosten" umzurechnen. Dies hat auch den Vorteil, dass Leser der Studie einen Kostenfaktor (in Euro) besser einordnen können als den Zeitaufwand (in Stunden).

F: Welche Faktoren sind in den Kosten, die in Unternehmen anfallen, enthalten?

A: Dazu gehören zunächst einmal die Gehälter derjenigen IT-Angestellten, die mit Malware zu tun haben, etwa indem sie die Probleme erkennen und beheben. Weitere Faktoren sind die Ausfallzeiten (IT und Endbenutzer) und externe Services. Hinzu kommt ein Anteil der Sicherheitskosten für die gesamte IT-Infrastruktur sowie die Kosten, die im Zusammenhang mit der Behebung von Datenpannen stehen.

F: Wie werden die Kosten, die im Zusammengang mit Datenpannen stehen, berechnet?

A: Zunächst einmal nutzen wir die vom Ponemon Institute veröffentlichten Informationen, anhand derer sich für einige wichtige Länder sowohl die durchschnittliche Größe einer Datenpanne als auch die Kosten, die bei der Wiederherstellung eines Datensatzes anfallen, ermitteln lassen. Anschließend gehen wir davon aus, dass eine von 1.000 Malwareinfektionen eine Datenpanne zur Folge hat. Während der Studie hat sich erwiesen, dass es sich hierbei um eine eher konservative Schätzung handelt.

F: Welche Möglichkeiten stehen Unternehmen offen, um die Sicherheitsrisiken zu minimieren?

A: Abgesehen davon, dass sie ausschließlich lizenzierte Original-Software einsetzen sollten, stehen Unternehmen zwei Möglichkeiten offen: 1) Unternehmen müssen dafür sorgen, dass alle Sicherheitsupdates zeitnah auf allen Systemen eingespielt werden. 2) Sie müssen eine Möglichkeit schaffen, um zu verhindern, dass Endanwender Software, die nicht vom Unternehmen bereitgestellt wurde, auf ihren Arbeits-PCs einspielen können. Eine überraschend hohe Anzahl von Unternehmen lässt sich mit der Installation von Sicherheitsupdates sehr viel Zeit. Die IDC-Studie zeigt, dass vom Endanwender unerlaubt eingespielte PC-Programme für rund 20% der Kosten, die Unternehmen bei der Behebung von Malwareinfektionen aufgrund raubkopierter Software aufwenden müssen, verantwortlich sind.

F: Was sehen Privatanwender und Unternehmen als größte Gefahr im Zusammenhang mit Malware an?

A: Ganz klar: Am meisten Sorgen machen sie sich über den Datenverlust und den unbefugten Datenzugriff durch Dritte.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com