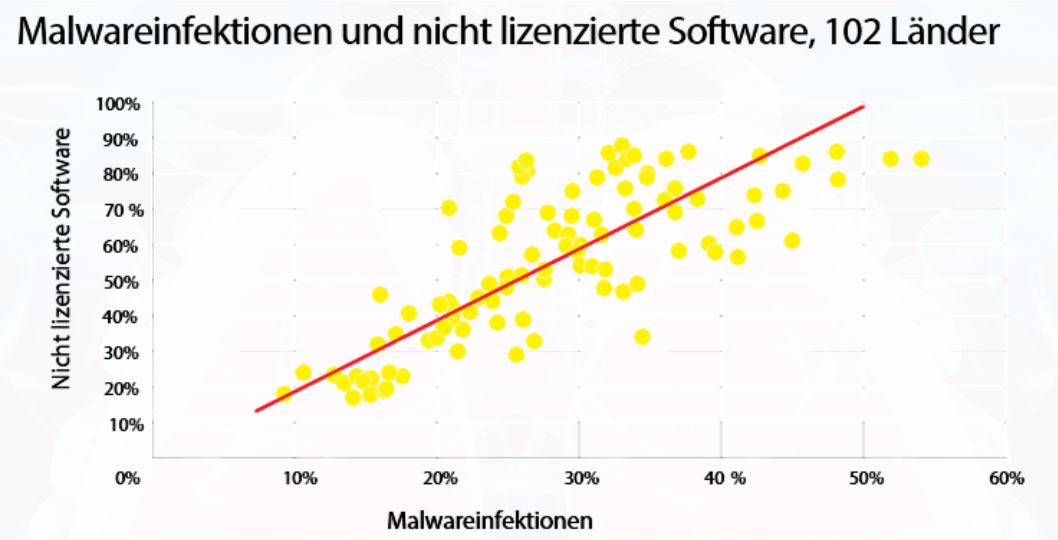
IDC INFOBRIEF ZUSAMMENFASSUNG

Wirtschaftliche Auswirkungen von Malwareinfektionen aufgrund der Nutzung raubkopierter Software (Europa, 2017)

November 2017
Gesponsert von Microsoft

Unübersehbare Korrelation: Malware und raubkopierte Software



Quelle: IDC 2017

- Das obige Diagramm basiert auf der Anzahl nicht lizenzierter Software (BSA, 2015) und den durchschnittlichen Malwareinfektionen je Quartal (2HJ2015 und 1HJ2016). Jeder Punkt steht für ein Land.
- Die Korrelation ist hoch – höher als der Zusammenhang zwischen Rauchen und Lungenkrebs (0,72).
- Das Bestimmtheitsmaß (R2) beträgt 0,60, was bedeutet, dass **60% der Malwareinfektionen im Zusammenhang mit nicht lizenzierter Software stehen**.
- Auch wenn eine Korrelation keine Kausalität bedingt, beweist die IDC-Studie, dass es in diesem Fall aber doch einen Zusammenhang gibt.

Grund der Korrelation: Häufigkeit von Malwareinfektionen durch raubkopierte Software

- Malware kann von der Website, von der die raubkopierte Software geladen wurde, stammen, sie kann im Programm selbst versteckt sein oder sie ist Bestandteil des illegitimen Aktivierungsschlüssels.
- Malware kann gefährliche Adware, Keylogger, die alle Tastatureingaben erfassen, Elemente zum Diebstahl von Passwörtern und anderen Zugangsdaten, Hintertüren für Hacker, sowie Software, die den Fernzugriff auf PCs ermöglicht, beinhalten.

Infektionsrisiko durch Raubkopien – unabhängig von den Quellen?

- **Eines von drei unlizenzierten oder raubkopierten PC-Softwareprodukten kann eine Malwareinfektion auslösen!**
- Das Risiko einer Malwareinfektion ist in allen Ländern und Segmenten nahezu gleich hoch.
- Die angegebenen Infektionsraten beziehen sich auf alle Quellen* – basierend auf IDC-Untersuchungen zur Softwaredistribution.
- In Europa** wird raubkopierte Software im Privatbereich dreimal häufiger genutzt als in Unternehmen. **Die Gesamtrate beträgt 28,6%, wobei Privatanwender auf 29,0% und Unternehmen auf 27,6% kommen.**

**Alle Quellen raubkopierter Software: auf dem PC vorinstalliert, aus dem Internet geladen (Web oder Filesharing) oder Installation mittels Medien.*
***Europa umfasst in diesem Fall alle west-, mittel- und osteuropäischen Länder.*

Malware-Einfallstor Nr. 1: Software aus dubiosen Quellen

- **66% aller europäischen Privatanwender** hatten Probleme mit Software, die aus dubiosen Quellen stammte – z.B. Online-Auktionen oder Online-Händler, von Freunden ausgeliehen, Straßenmärkte.
- **69% aller in Europa innerhalb der letzten beiden Jahre von Privatanwendern gekauften PCs** stammten ebenfalls aus „riskanten" Quellen – z.B. Berater, Online-Tauschbörsen, Geschenke, PC-Schrauber.
- **33% aller in Unternehmen verwendeten PCs** stammten aus dubiosen Quellen.

Malware-Einfallstor Nr. 2: Nachlässiger Umgang mit Sicherheitsupdates

- Die Gründe für den nachlässigen Umgang mit Sicherheitsupdates reichen von der Angst, dass die Nutzung raubkopierter Software entdeckt wird, bis hin zu fehlenden Richtlinien und Prozessen.
- Gefährlich sind insbesondere sogenannte Zero-Day-Exploits, also neu entdeckte Sicherheitslücken, die erst nach einigen Tagen durch Patches geschlossen werden. **Dennoch finden zwei Drittel der Malwareinfektionen NACH der Bereitstellung von Updates statt.**

Infizierte Raubkopien: Davor fürchten sich europäische Privatanwender

Top-4-Ängste

1. Verlust von Daten, Dateien oder privaten Informationen **51%**
2. Diebstahl und Missbrauch von E-Mail-Konten, sozialen Netzwerken und Online-Banking **47%**
3. Unerlaubte Transaktionen und Online-Betrug **41%**
4. Möglicher Identitätsdiebstahl **37%**

Infizierte Raubkopien: Davor fürchten sich europäische Unternehmen

Top-4-Ängste

1. Datenverlust **45%**
2. Zeitaufwand und Kosten, die bei der Desinfektion anfallen **38%**
3. Systemversagen und Ausfallzeiten **31%**
4. Verlust geistigen Eigentums und sensibler Informationen **24%**

Kosten, die europäischen Privatanwendern durch Nutzung infizierter Software entstehen: 7,2 Milliarden Euro, 319 Millionen Stunden!

- Zeit und Geld müssen in die Identifizierung, Reparatur, Datenwiederherstellung und die Auswirkungen von Identitätsdiebstahl und Ransomware investiert werden.
- Die Arbeitskosten basieren auf dem durchschnittlichen Stundenlohn im jeweiligen Land (Wechselkurs 2016).
- **Insgesamt müssen 319 Millionen Stunden investiert werden. Das entspricht in etwa 10 Stunden pro infizierter Software oder 231 Euro.**

Kosten, die europäischen Unternehmen durch Nutzung infizierter Software entstehen: 51 Milliarden Euro!

- Zeit und Geld müssen in die Identifizierung, Reparatur, Datenwiederherstellung und die Auswirkungen von Ransomware investiert werden. Einige Arbeiten werden intern durchgeführt, andere werden von externen Spezialisten erledigt.
- Die Arbeitskosten basieren auf dem durchschnittlichen IT-Stundenlohn im jeweiligen Land (Wechselkurs 2016).
- **Die Gesamtkosten betragen 6.220 Euro für jede infizierte Einheit.** Die Kosten beinhalten IT-Arbeit, Kosten für externe Dienstleistungen, einen Anteil am IT-Gesamtbudget sowie die im Zusammenhang mit verlorenen Daten stehenden Ausgaben.

IDC empfiehlt

- Erwerben Sie Ihre PCs und Software ausschließlich bei vertrauenswürdigen Quellen.
- Nutzen Sie keine unlizenzierte Software oder Raubkopien – stellen Sie sicher, dass die verwendete Software legal ist.
- Installieren Sie zuverlässige Sicherheitslösungen.
- Achten Sie auf alle neuen Sicherheitsupdates – Ignorieren ist keine Lösung.
- Überwachen Sie regelmäßig, welche Software Ihre Mitarbeiter installieren.
- Legen Sie Sicherungen von allen wichtigen Dateien an – im Idealfall werden die Backups in Echtzeit durchgeführt.
- Bezahlen Sie niemals das von Cyber-Kriminellen, die Ransomware verbreiten, geforderte „Lösegeld" – Gangstern kann man nicht vertrauen.

ÜBER DIESE PUBLIKATION
Diese Publikation wurde von IDC Custom Solutions verfasst. Die in diesem Dokument veröffentlichten Meinungen, Auswertungen und Forschungsergebnisse basieren auf detaillierten Analysen und Untersuchungen, die von IDC auf unabhängige Art und Weise durchgeführt und veröffentlicht wurden. Sofern Sponsoren involviert sind, wird darauf hingewiesen. IDC Custom Solutions stellt Inhalte, die von IDC produziert werden, in verschiedenen Formaten zur Verfügung, sodass sie von diversen Unternehmen distribuiert werden können. Die Lizenz, IDC-Inhalte zu distribuieren, impliziert weder die Befürwortung des Lizenznehmers, noch dass seine Meinung geteilt wird.

URHEBERRECHT UND EINSCHRÄNKUNGEN
Alle von IDC stammenden Informationen sowie Verweise auf IDC, die in Werbemitteln, Pressemeldungen oder verkaufsfördernden Materialien verwendet werden, erfordern eine vorherige schriftliche Genehmigung von IDC. Wenden Sie sich dazu telefonisch oder per E-Mail (gms@idc.com) an Custom Solutions. Die Übersetzung und/oder Lokalisierung dieses Dokuments setzt eine weitere Lizenz von IDC voraus.

Weitere Informationen erhalten Sie auf www.idc.com. Mehr zu IDC Custom Solutions finden Sie auf der Webseite http://www.idc.com/prodserv/custom_solutions/index.jsp.

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