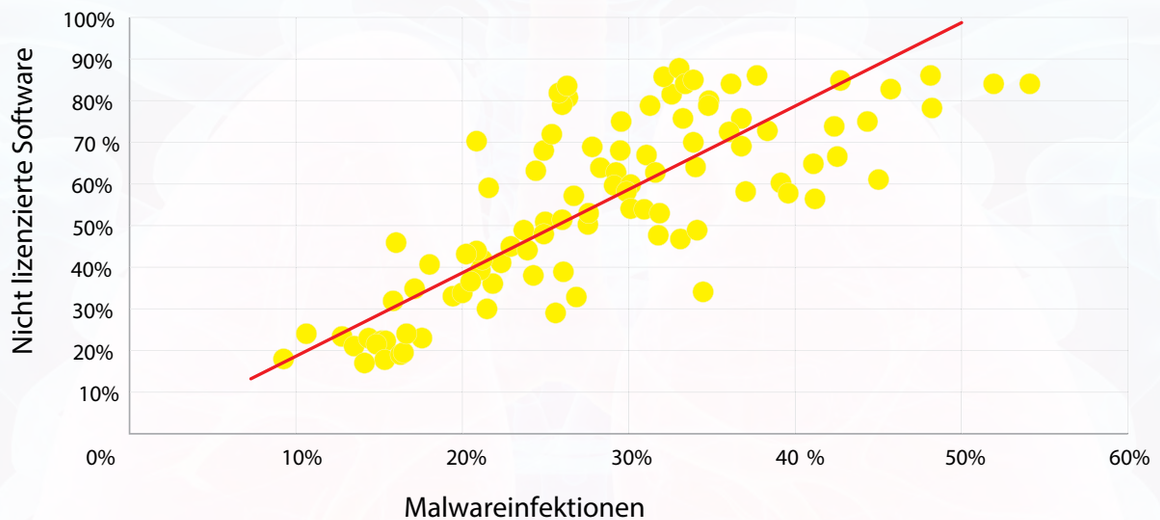
Sicherheitsrisiko Raubkopien: Ursachen, Kosten und Gefahren

Eine IDC-Studie, gesponsert von Microsoft | September 2017

IDC
ANALYZE THE FUTURE

Unübersehbare Korrelation: Malware und raubkopierte Software

Malwareinfektionen und nicht lizenzierte Software, 102 Länder



- Die Korrelation ist hoch – höher als der Zusammenhang zwischen Rauchen und Lungenkrebs (0,72).
- Das Bestimmtheitsmaß (R^2) 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.

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.

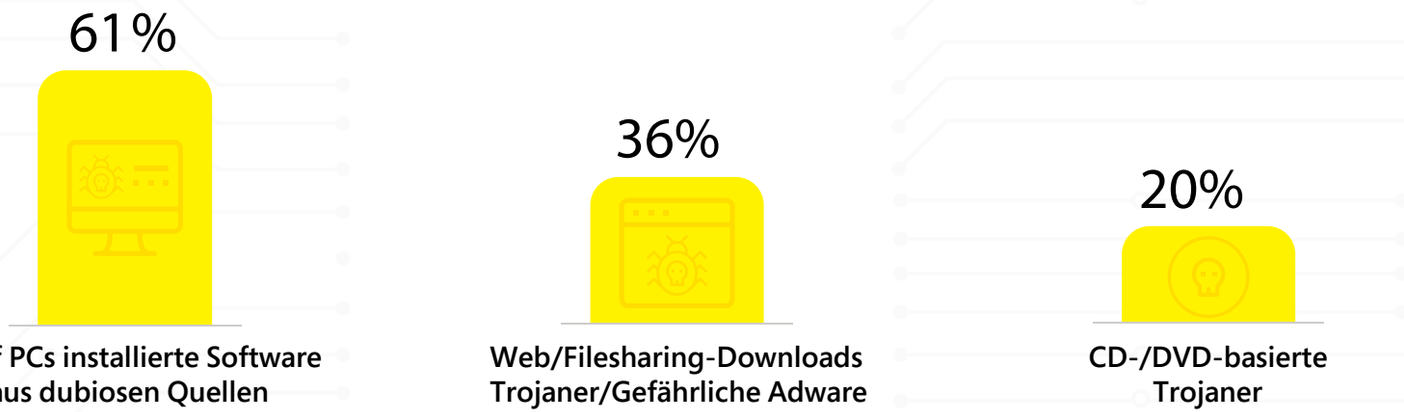
Referenzen:

BSA report "Unlicensed Software and Cybersecurity Threats," Januar 2015 (http://globalstudy.bsa.org/2013/malware/study_malware_en.pdf)

The New York Times, "China, Addicted to Bootleg Software, Reels from Ransomware Attack", 15. Mai 2017 (https://www.nytimes.com/2017/05/15/business/china-ransomware-wannacry-hacking.html?_r=0)

Grund der Korrelation: Häufigkeit von Malwareinfektionen durch raubkopierte Software

Infektionsraten basierend auf den Quellen der Raubkopien



» 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.

Basierend auf einer von IDC durchgeführten Längsschnittstudie, die sich mit dem Infektionsrisiko von Raubkopien und Aktivierungsschlüsseln, die aus dem Web/per Filesharing geladen wurden, befasste. Zusätzliche Daten stammen aus einer von der National University of Singapore durchgeführten Analyse von Laptops, die mit vorinstallierten Raubkopien erworben wurden.

Referenzen:

IDC White Paper "The Link between Pirated Software and Cybersecurity Breaches," März 2014 (http://download.softwareculicenta.ro/raport-idc-2014-03.pdf)

Symantec report, "Underground Black Market: Thriving Trade in Stolen Data, Malware, and Attack Services," November 2015 (https://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services)

Infektionsrisiko durch Raubkopien – unabhängig von den Quellen?

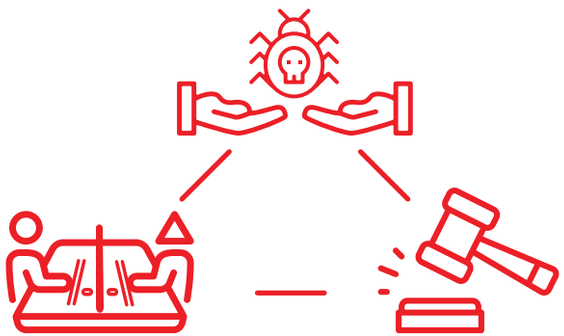
Wahrscheinlichkeit von Malwareinfektionen durch Raubkopien (Europa, 2017)

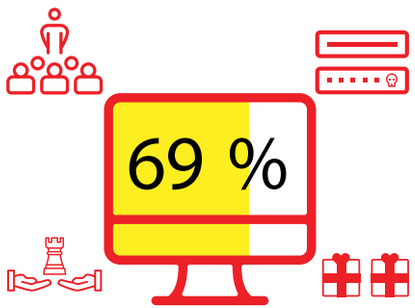
Alle Quellen raubkopierter Software: auf dem PC vorinstalliert, aus dem Internet geladen (Web oder Filesharing) oder Installation mittels Medien.

- 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.

Eines von drei unlizenzierten oder raubkopierten PC-Softwareprodukten kann eine Malwareinfektion auslösen!

Malware-Einfallstor Nr. 1: Software aus dubiosen Quellen





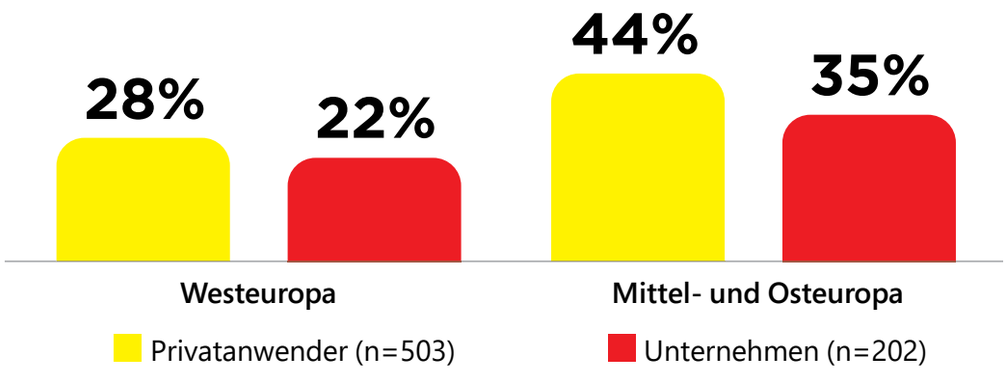
» 66% aller europäischen Privatanwender hatten Probleme mit Software, die aus dubiosen Quellen stammte – z.B. Online-Auktionen oder Online-Händler, von Freunden ausgeliehen, Straßenmärkte.

» 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

Wahrscheinlichkeit von Malwareinfektionen durch Raubkopien (Europa, 2017)



» 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.

» Zwei Drittel aller Malwareinfektionen finden nach der Bereitstellung von Updates, die jedoch nicht eingespielt wurden, statt.

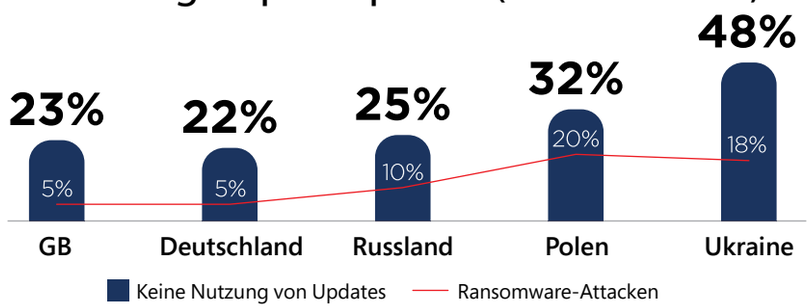
Referenzen:

Business Insider Artikel, "The New Global Ransomware Attack Shows How Many People Still Don't Install Software Updates", 28. Juni 2017 (http://www.businessinsider.com/people-still-dont-install-software-updates-2017-6)

ZDNet Artikel, "Seven Myths about Zero Day Exploits Debunked," 3. August 2010 (http://www.zdnet.com/article/seven-myths-about-zero-day-vulnerabilities-debunked/)

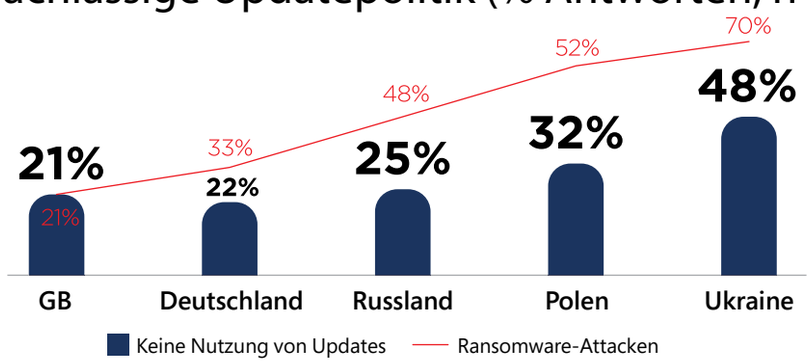
Die Folgen einer nachlässigen Updatepolitik: Ransomware-Attacken

Ransomware-Attacken und nachlässige Updatepolitik (% Antworten, n=202)



- Die Korrelation zwischen Ransomware-Attacken und nachlässiger Updatepolitik ist hoch (0,79).
- Die Gründe für den nachlässigen Umgang mit Sicherheitsupdates reichen von „das ist viel zu stressig“ bis hin zur Angst, dass die Nutzung raubkopierter Software entdeckt wird.
- Die Korrelation zwischen Softwareproblemen ist sogar noch höher (0,91).

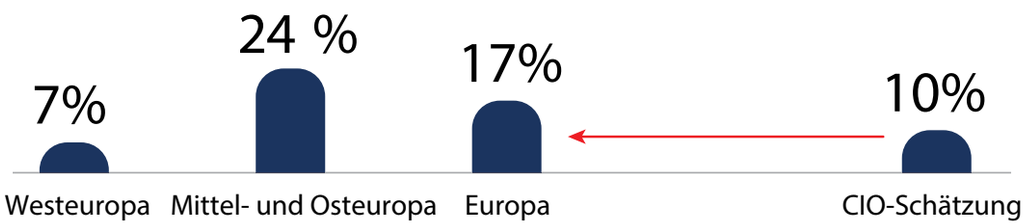
Dubiose Software* und nachlässige Updatepolitik (% Antworten, n=202)



*Office auf PCs vorinstalliert

Das Trojanische Pferd der Malwareinfektionen: Bring Your Own Software

Anteil der Mitarbeiter, die innerhalb der letzten beiden Jahre unerlaubt Software auf den Unternehmens-PCs installiert haben (n=369)

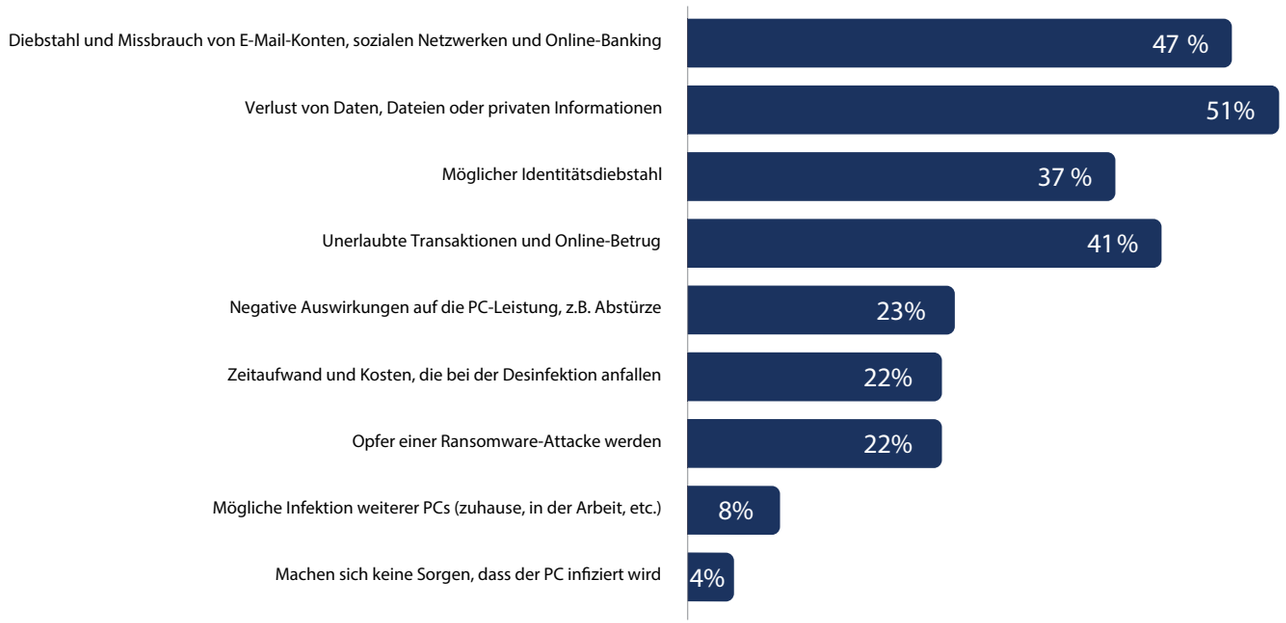


- CIOs unterschätzen die Anzahl der Mitarbeiter, die eigene Software auf Unternehmens-PCs installieren.
- Knapp 50% der europäischen Unternehmen überprüfen die von Mitarbeitern verwendete Software maximal zweimal im Jahr. Weniger als die Hälfte der Unternehmen verfügen über offizielle Richtlinien, die die Softwareinstallation durch Benutzer auf Arbeits-PCs regeln.
- BYOSW ist teuer: 17% der europäischen Arbeitnehmer installieren – ohne Wissen des Unternehmens – Software auf Arbeits-PCs. Bei einem Großteil der Programme handelt es sich um unlizenzierte und somit potenziell gefährliche Software. Die Folge: BYOSW erhöht die Gefahr, dass Unternehmens-PCs von Malware infiziert werden, um 19%.

Das Vorhandensein von Prozessen, die die Installation von BYO-Software auf Unternehmens-PCs regeln, stellt eine eminent wichtige Schutzmaßnahme vor Malware dar.

Infizierte Raubkopien: Davor fürchten sich europäische Privatanwender

Infizierte Raubkopien: Die größten Ängste der Privatanwender (% Antworten, n=503)

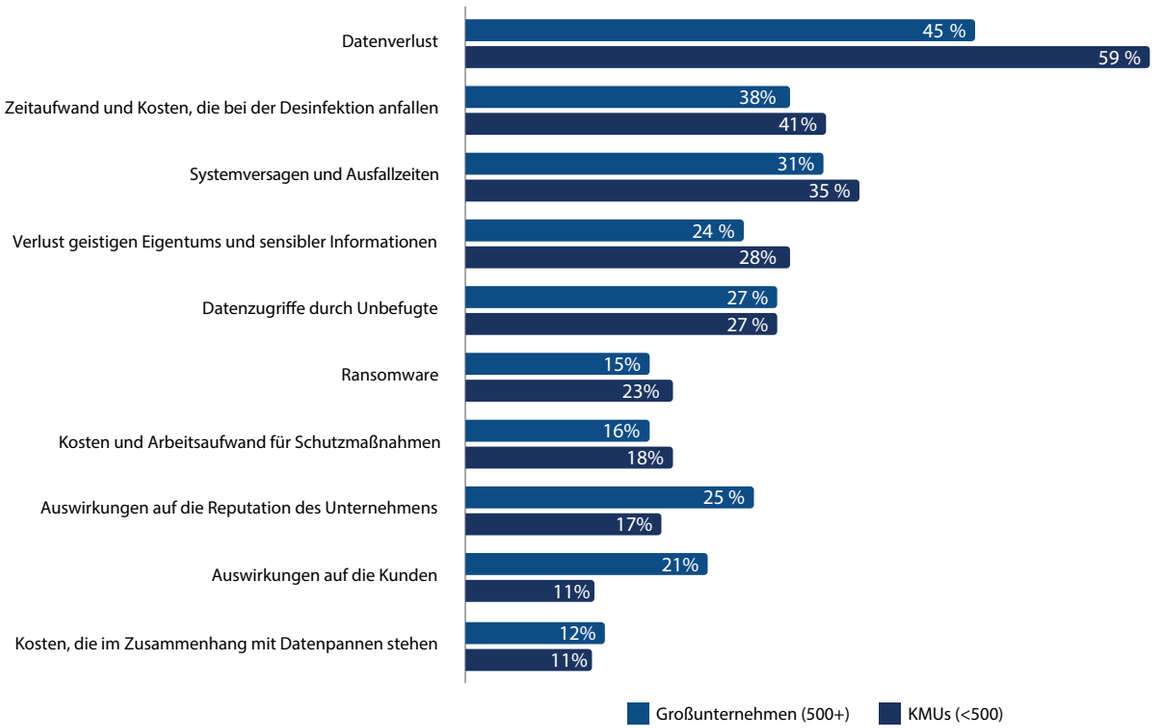


96% aller Privatanwender machen sich Sorgen, dass die Nutzung von Raubkopien oder unsachgemäß lizenzierter Software zu Malwareinfektionen führt.

(Unsachgemäß lizenziert bedeutet in diesem Fall, dass eine Software mit Einzelplatzlizenz auf mehreren Geräten verwendet wird.)

Infizierte Raubkopien: Davor fürchten sich europäische Unternehmen

Infizierte Raubkopien: Die größten Ängste der Unternehmen (% Antworten, n=202)

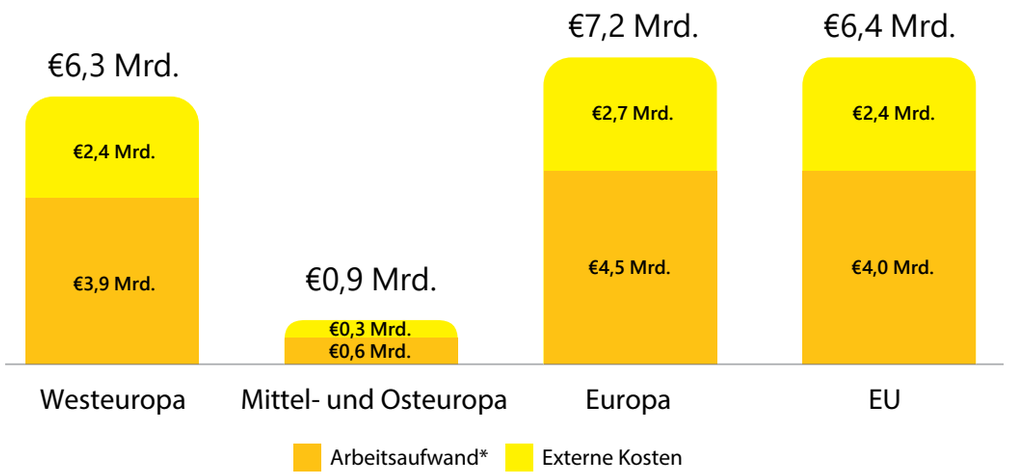


- 16% erlebten bereits eine Datenpanne, der Durchschnitt: 3,7 Datenpannen; durchschnittliche Datenpanne: 2.900 Aufzeichnungen.
- In Mittel- und Osteuropa kommen Datenpannen 2,5 Mal häufiger vor als in Westeuropa. Allerdings ist die Anzahl der verlorenen Dateien in Westeuropa fünf Mal höher.
- 11% wurden bereits Opfer von Ransomware, der jährliche Durchschnitt beträgt 4,1. Durchschnittlich betrug die Ransomware-Forderung 1.395 US-Dollar, allerdings bezahlten nur 18% der Befragten.
- Viele Unternehmen konnten ihre Daten auch ohne Bezahlung retten, etwa durch das Einspielen einer Datensicherung oder mithilfe von Tools, die die verschlüsselten Dateien entschlüsselten. So bietet Microsoft etwa mit Windows Defender Online ein solches Hilfsmittel an, andere Hersteller offerieren ebenfalls interessante Lösungen.

Datenverluste und –pannen spielen die größten Rollen.

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

Durch in Raubkopien enthaltene Malware verursachte Kosten für Privatanwender (Europa 2017)



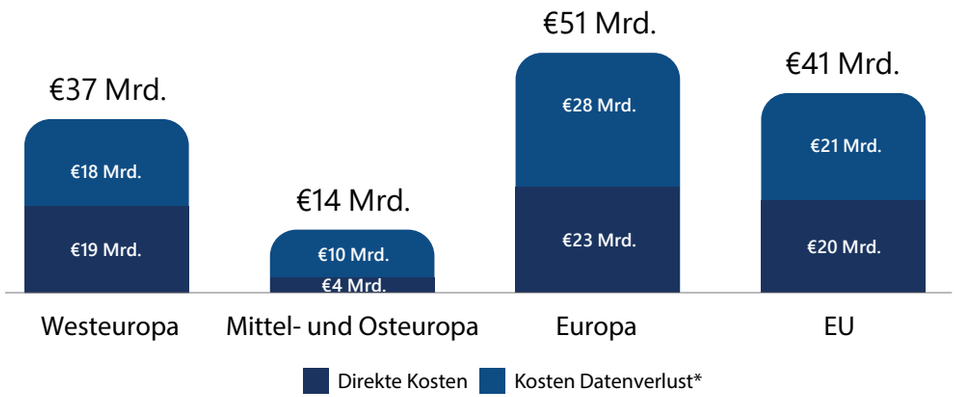
*Arbeitskosten basieren auf dem durchschnittlichen Stundenlohn 2017

- Zeit und Geld müssen in die Identifizierung, Reparatur, Datenwiederherstellung und die Folgen 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.
- Diese Analyse basiert auf Durchschnittswerten, sodass die Kosten in Einzelfällen signifikant höher sein können. Beispiel: US-Statistiken zufolge hat die Hälfte der Personen, die Opfer eines Identitätsdiebstahls wurden, das Problem nach einem Tag gelöst. Bei 10% der Personen zieht sich die Lösung allerdings länger als einen Monat hin.

Die bei einer Infektion anfallenden Kosten können den Preis der Original-Software um ein Vielfaches übersteigen.

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

Durch in Raubkopien enthaltene Malware verursachte Kosten für Unternehmen (Europa 2017)



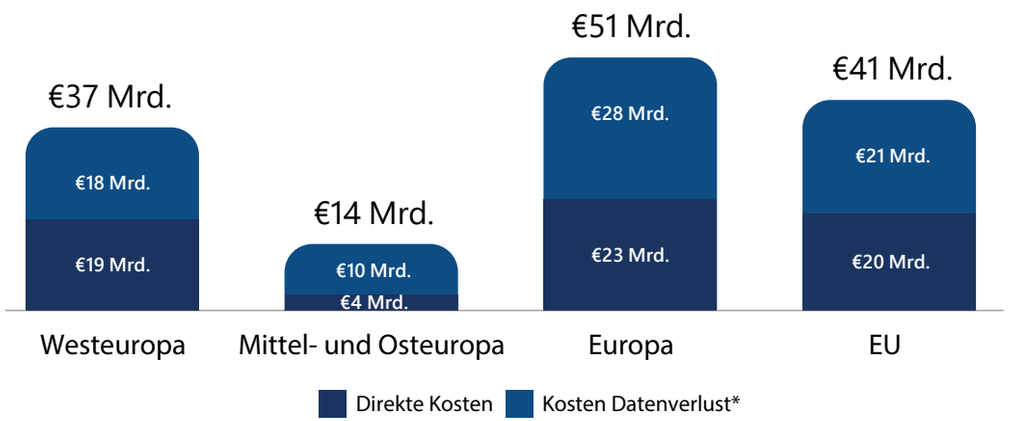
*Davon ausgehend, dass eines von 1.000 infizierten Softwareprodukten zu einer Datenpanne führt.

- Zeit und Geld müssen in die Identifizierung, Reparatur, Datenwiederherstellung und die Folgen 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, externe Dienstleistungen, einen Anteil am IT-Gesamtbudget sowie die im Zusammenhang mit verlorenen Daten stehenden Ausgaben.
- Die beim Datenverlust anfallenden Kosten basieren auf der Schätzung, dass es bei einem von 1.000 infizierten Softwareprodukten zu einer Datenpanne kommt.
- Die beim Datenverlust anfallenden Kosten umfassen die Behebung (Problem finden und lösen), die Folgen für die Kunden, Bußgelder, Ausgaben für Rechtsberatung sowie den Verdienstausfall. Nicht mit einberechnet ist der Diebstahl extrem sensibler Informationen (z.B. geheime Forschungsergebnisse und ähnliches geistiges Eigentum).

Die bei einer Infektion anfallenden Kosten können den Preis der Original-Software um ein Vielfaches übersteigen.

Kleinen und mittelständischen Unternehmen entstehen durch Nutzung infizierter Software die höchsten Kosten

Durch in Raubkopien enthaltene Malware verursachte Kosten für Unternehmen (Europa 2017)



*Davon ausgehend, dass eines von 1.000 infizierten Softwareprodukten zu einer Datenpanne führt.

- Die in KMUs bereitgestellte Software macht zwar weniger als 50% aller in Unternehmen genutzten PC-Programme aus, allerdings ist der Anteil von Raubkopien größer als 50%.
- Aufgrund des salopperen Umgangs mit Sicherheitsupdates, kommen rund 60% aller infizierten Raubkopien in KMUs zum Einsatz.
- Kleinunternehmen sind wiederum für 60% der KMU-Gesamtkosten verantwortlich.

Je kleiner ein Unternehmen ist, desto größer die Gefahr,
dass mit Malware infizierte Raubkopien zum Einsatz kommen.

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.