AVG Business

Behalten Sie die Kontrolle über Ihr Unternehmen

Ransomware: Fakten, Zahlen und Merkmale

Eine steigende Anzahl kleiner und mittlerer Unternehmen (KMU) werden Opfer von Ransomware, einer Schadsoftware, durch die Lösegeld für Ihren Computer und die Daten gefordert wird. Nicht alle KMUs kennen die Risiken und Auswirkungen auf ihr Unternehmen.

Ransomware dringt weiter vor

400.000.000
Varianten von Ransomware insgesamt, 1.200.000 neue Varianten in 2015

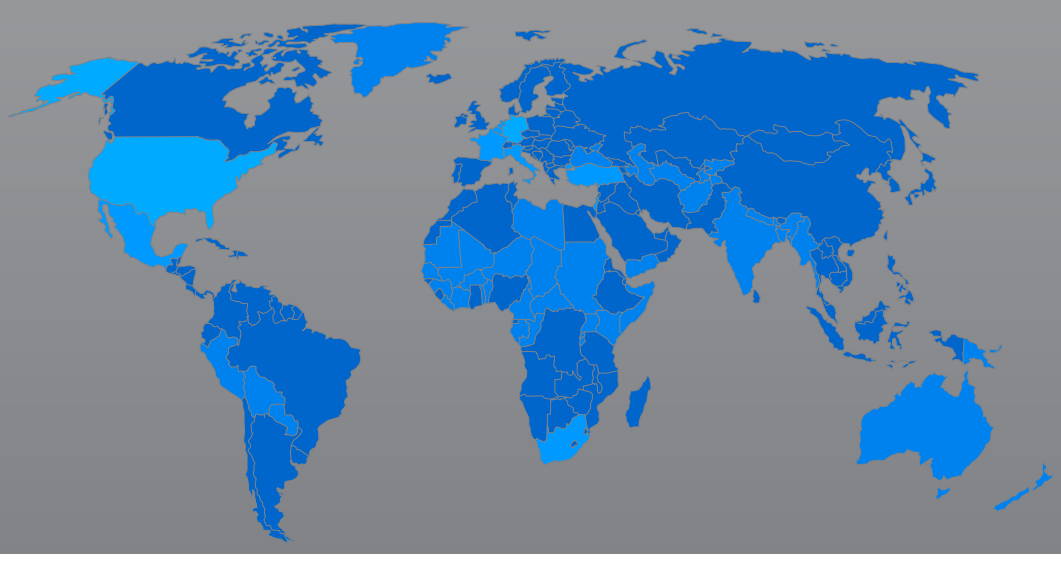
60.000
neu mit Locky infizierte Computer innerhalb von 24 Stunden

325.000.000
US-Dollar
Schaden weltweit durch eine Ransomware-Variante (CryptoWall)

200-10.000
US-Dollar
als Lösegeldforderung

27.000.000
US-Dollar
Lösegeld gezahlt in der nicht nachverfolgbaren Währung Bitcoin

Weltweite Verbreitung der von Locky infizierten Computer



16.500	in Deutschland
10.900	in den USA
5.200	in Italien
5.000	in den Niederlanden
4.300	in Südafrika
4.100	in Frankreich
3.200	in Belgien
2.900	in Israel
2.800	in der Türkei
2.300	in Mexiko

„Dies giltnicht für mein Unternehmen, oder?“

Doch, sehr wohl. KMUs sind ein beliebtes Ziel.

80%
Nach einer weltweiten Studie verwenden 80% der KMUs keinen Datenschutz

50%
Nur die Hälfte der KMUs verwendet E-Mail-Schutz, obwohl Ransomware überwiegend über E-Mail verbreitet wird

4/10
Wahrscheinlichkeit, dass Mitarbeiter auf schädliche Links in E-Mails klicken, ist in KMUs viermal größer

Ransomware-Angriffe haben erheblich negative Auswirkungen auf kleine und mittlere Unternehmen (KMU), da sie nicht immer für das Lösegeld oder die durch den Schaden verursachten Kosten aufkommen können.

Eine Bedrohung für die Betriebszeit von Unternehmen

Im betrieblichen Umfeld gilt, dass Zeit Geld ist. Eine Umfrage unter 300 Personen in Unternehmen jeder Größenordnung hat gezeigt, dass die Ausfallzeit während und nach eines Angriffs mehr Schaden anrichten kann, als der Angriff selbst.

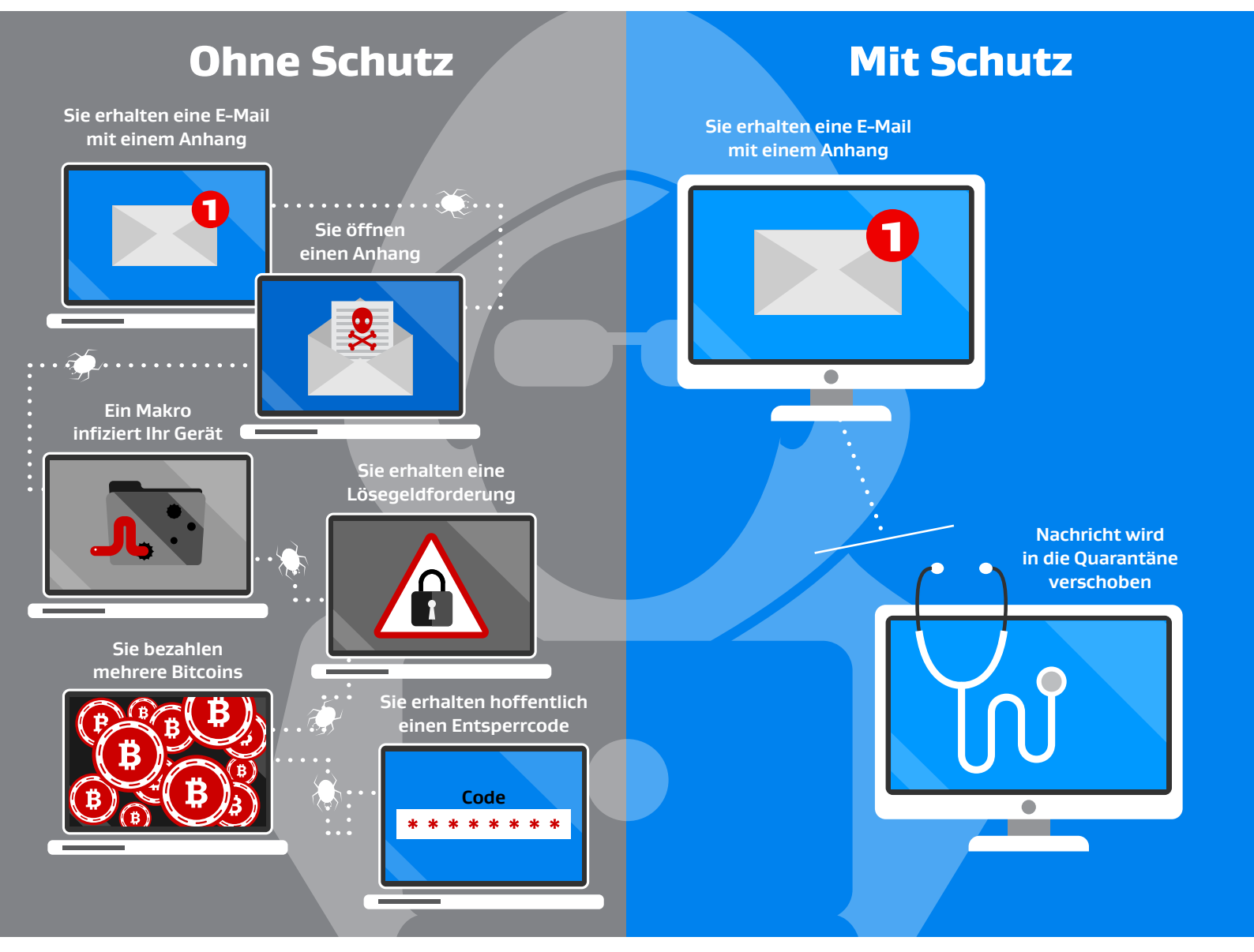
72 Stunden
ist die durchschnittliche Zeit, die das Opfer zum Zahlen des Lösegelds hat

72%
ist der Prozentsatz der infizierten Unternehmen, die mindestens zwei Tage nach einem Ransomware-Angriff nicht auf ihre Daten zugreifen können

32%
der Betroffenen hatten mindestens fünf Tage lang keinen Zugriff

Wie funktioniert Ransomware?

Die folgende Abbildung zeigt, wie Ransomware es schafft, Ihr Unternehmen zu erpressen. Diese Abbildung basiert auf der berüchtigten Ransomware „Locky“.



Behalten Sie die Kontrolle über Ihr Unternehmen

Rufen Sie www.avg.com/business-security auf oder wenden Sie sich an Ihren autorisierten AVG Business Security-Partner

#securitysimplified

Quellen:
http://bit.ly/1Wx0wRw
http://bit.ly/207ZAoV
http://bit.ly/23NGDOb
http://on.wsj.com/1FOVvu0
http://bit.ly/1jdOzCI
http://bit.ly/1TmJc12
http://bit.ly/1SgbXh9

The Online Security Company™
Devices. Data. People.™