



dimension data

accelerate your ambition

# Ransomware: Allgegenwärtige Gefahr für Unternehmen

Eine Infografik von Frost & Sullivan, im Auftrag von Dimension Data und Cisco

## Wie funktioniert Ransomware?

Ransomware ist ein *Schadprogramm*, das *Dateien auf Computern und Servern des Opfers verschlüsselt* und Geld dafür verlangt, diese wieder zu entschlüsseln. Hierfür *nutzt das Programm Schwachstellen im Betriebssystem*. Die Attacken verursachen oft *massive Betriebsstörungen* und können für Cyberkriminelle eine lukrative Einnahmequelle darstellen.

## Schäden durch Ransomware



Quellen: \* Cisco 2017 Mid-Year Cyber Security Report | \*\* FBI | \*\*\* Los Angeles Times

## Ein leichtes Ziel: Welche Unternehmen gefährdet sind

Betroffene Unternehmen machen folgende Fehler bei der IT-Sicherheit:



Kein vorhandenes Patch-Management



Ineffektive Vorkehrungen gegen die Infizierung mit und die Verbreitung von Malware



Mangel an Einrichtungen für Backups und Datenwiederherstellung

## Wie sich Unternehmen gegen Ransomware schützen können



## Schlüsselfragen für eine Strategie zur Abwehr von Ransomware

- Wann** wurde die Sicherheit des IT-Systems in Ihrem Unternehmen zuletzt geprüft? Kennen Sie Ihre Vorteile und Schwachstellen?
- Haben** Sie Ihre Sicherheitslösungen und deren Effektivität hinsichtlich Ransomware-Attacken überprüft?
- Ist** Ihre Netzwerkinfrastruktur in der Lage, die Sicherheit zu verbessern?
- Verfügen** Sie über eine vielschichtige Strategie, die verschiedene Sicherheitslösungen und -services kombiniert, um Ransomware zu stoppen?
- Sind** Backups und Datenwiederherstellung Teil Ihrer Strategie?

Erfahren Sie, wie Sie Ihr Unternehmen gegen Krisen wappnen und den Betrieb während einer Ransomware-Attacke möglichst aufrecht erhalten können unter [www.dimensiondata.com/ransomware](http://www.dimensiondata.com/ransomware)