Ransomware ist Realität

Sie ist zur **profitabelsten Art von Malware** für Cyber-Diebe geworden!

Mehr als 40 % der Opfer zahlen das Lösegeld

40 % aller Unternehmen weltweit haben im letzten Jahr mit Ransomware zu tun gehabt

Allein in den USA verzeichneten 50 % aller Unternehmen einen Ransomware-Vorfall

Bei 60 % der Erpressungsangriffe auf Unternehmen wurden 1000 $ oder mehr verlangt

Malware-Landschaft entwickelt sich ständig weiter

- **Ausgeklügelter**
- **Besser organisiert**
- **Teurer**

- **VERLUST SENSITIVER DATEN**
- **SCHWERE FINANZIELLE VERLUSTE**
- **MASSIVE BETRIEBS-STÖRUNG**
- **RUF-SCHÄDIGUNG**

Sagen Sie Cyber-Dieben den Kampf an!

Ingram Micro und **Cisco** helfen Ihnen, Gefahren zu erkennen und zu bekämpfen.

Malware **verschlüsselt** und speichert **wichtige Dokumente und Dateien,** bis Unternehmen ein **Lösegeld zahlen,** um die Dateien zu entschlüsseln und zurückzubekommen.

Anatomie eines Angriffs

Wie ein Angriff abläuft

INFEKTIONS-VEKTOR
Nutzer klickt auf einen schädlichen Link

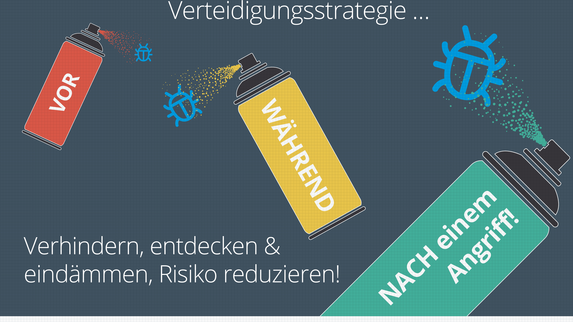
DATEN NUTZEN SYSTEM AUS
Ransomware-Datei wird heruntergeladen

SCHLÜSSELAUSTAUSCH
Rückruf an schädliche Ransomware-Infrastruktur

VERSCHLÜSSELUNG VON DATEIEN
Möglichst viele Dateien werden infiziert

LÖSEGELD-FORDERUNG
Nach Verschlüsselung wird die Lösegeldforderung angezeigt

Angriffsprävention mit unserer vielschichtigen Verteidigungsstrategie ...



Verhindern, entdecken & eindämmen, Risiko reduzieren!

Erfahren Sie, was Ingram Micro und Cisco für Sie tun können!

IHREN EXPERTEN KONTAKTIEREN

Oder besuchen Sie **www.ingramflyhigher.com/de/landing-pages/ransomware** um mehr zu erfahren