Acronis

10 einfache Tipps zum Schutz Ihres Unternehmens vor Ransomware

Ransomware-Angriffe auf Unternehmen und Institutionen sind aktuell die häufigste Art von Malware-Vorfällen. Sie machen immerhin 39% aller IT-Sicherheitsvorfälle aus – und nehmen ständig zu! Die geschätzten Einnahmen der Ransomware-Kriminellen sollen sich bis 2019 auf ca. 10 Milliarden Euro belaufen. Aber mit ein paar einfachen Richtlinien und Prozeduren sowie einigen innovativen Gegenmaßnahmen auf den Endgeräten/Endpunkten können Sie Ihr Unternehmen effektiv vor der Ransomware-Bedrohung schützen.

1

Halten Sie Ihre Betriebssysteme und Applikationen auf dem neuesten Stand
Ransomware-Angriffe (wie der bekannte WannaCry-Ausbruch von 2017) nutzen üblicherweise Software-Schwachstellen aus, die zumeist durch Installation der neuesten Updates und Sicherheitspatches für die eingesetzten Betriebssysteme und Applikationen geschlossen werden könn(t)en. Unternehmen, die auf Microsoft Windows setzen, sollten beispielsweise regelmäßig die Microsoft Security Bulletins verfolgen, um über die neuesten Sicherheits-updates für Windows im Bilde zu sein.

2

Führen Sie regelmäßige Backups durch
Regelmäßige, vollständige Image-Backups sind die zuverlässigste Methode, um sich gegen Ransomware-Angriffe zu schützen. Wenn Sie unternehmenskritische Dateien regelmäßig sichern – am besten sowohl zu einem lokalen Storage als auch zu einem sicheren Cloud Storage – können Sie die Auswirkungen eines Ransomware-Angriffs jederzeit zurückdrehen, indem Sie betroffene Systeme auf den Zustand davor zurücksetzen. Vielleicht verliert Ihr Unternehmen dennoch einige Daten und Dateien, die seit dem letzten Backup erstellt wurden. Aber Ihre Systeme werden schnell wieder betriebsbereit sein und Sie müssen kein Lösegeld zahlen.

3

Installieren Sie eine Anti-Virus-Software und halten Sie deren Signatur-Datenbank aktuell
AV-Produkte (Antivirus) für Endgeräte bieten einen wertvollen Schutz gegen viele gängige Malware-Angriffe. Unternehmen sollten Ihr AV-Produkt sorgfältig auswählen und deren Signatur-Datenbank möglichst automatisch aktualisieren lassen.

4

Aktivieren Sie Acronis Active Protection in Acronis Backup
Weil viele neue Ransomware-Varianten einen herkömmlichen AV-Schutz jedoch umgehen können, sollte Ihr Unternehmen auch eine moderne Data Protection-Software mit integrierter Anti-Ransomware-Funktion bereitstellen, wie sie Acronis Backup mit Active Protection bieten kann. Diese innovative Technologie arbeitet mit heuristischer Verhaltenserkennung und maschinellem Lernen, um Ransomware-Angriffe automatisch zu erkennen, zu stoppen und dennoch betroffene Dateien automatisch wiederherzustellen.

5

Schließen Sie bekannte Schwachstellen in Ihrem Unternehmens-E-Mail-System

Ihr E-Mail-Administrator kann einige einfache Konfigurationsänderungen für alle Anwender vornehmen, durch die mögliche Ransomware-Angriffe offensichtlicher werden. Machen Sie beispielsweise Dateinamenserweiterungen (wie .pdf für Adobe Reader-Dokumente) standardmäßig sichtbar. Ihre Mitarbeiter können so potentiell gefährliche Dateianhänge (wie ausführbare JavaScript-Dateien mit der Dateierweiterung .js) leichter erkennen, die sich sonst z.B. als harmlose Word-Dokumente (.docx) tarnen. Sie sollten auch erwägen, standardmäßig alle E-Mail-Anhänge unternehmensweit auf Viren zu scannen.

6

Unterrichten Sie Ihre Anwender darin, kein Ransomware-Opfer zu werden

Phishing-E-Mails, die sich mit persönlichen Informationen aus Quellen wie Facebook und LinkedIn als vertrauenswürdig ausgeben, sind häufige Vektoren für Ransomware-Angriffe. Trainieren Sie Ihre Kollegen darauf, E-Mails aus Quellen, die nicht explizit bekannt und absolut vertrauenswürdig sind, zu misstrauen. Sensibilisieren Sie Ihre Mitarbeiter für das Risiko, auf E-Mail-Links zu klicken und E-Mail-Anhänge zu öffnen. Und ermutigen Sie Ihre Mitarbeiter, bei verdächtigen E-Mails den Absender zu kontaktieren.

7

Segmentieren Sie das Unternehmensnetzwerks, um Wurm-Ausbreitungen einzudämmen

Viele Ransomware-Varianten können sich, von einer zuerst kompromittierten Maschine ausgehend, dann auf andere Server und PCs im Netzwerk ausbreiten. Erschweren Sie diese Art der Verbreitung, indem Sie Ihre Unternehmensnetzwerk durch Technologien wie Zugriffssteuerungslisten (ACLs), private VLANs und kontextbezogene sichere Segmentierung unterteilen.

8

Gewähren Sie nur solchen Benutzern und Applikationen administrative Rechte, die diese wirklich benötigen

Je mehr Berechtigungen ein Benutzer oder eine Applikation hat, desto größer ist das Schadenspotenzial, wenn diese Berechtigungen kompromittiert werden. Vergeben Sie standardmäßig nur Basisrechte und seien Sie zurückhaltend, höhere Berechtigungsstufen über die Benutzerkontensteuerung zu gewähren.

9

Aktivieren Sie die neuesten Sicherheitsfunktionen in Ihren Unternehmens-applikationen

Beliebte Business-Applikationen (wie Microsoft Office) enthalten nun viele standardmäßig blockierende Sicherheitsfunktionen, z.B. dass Makro-Ausführungen bei Word- und Excel-Dokumenten deaktiviert sind. Übernehmen Sie diese Voreinstellungen unternehmensweit, um weitere Angriffsvektoren zu schließen, die häufig von Ransomware verwendet werden.

10

Erlauben Sie keine Programmstarts aus den Systemordnern „AppData" und „LocalAppData"

Viele Ransomware-Varianten versuchen, sich durch eine Ausführung aus bestimmten System-Ordnern heraus als Standard-Windows-Prozess zu maskieren. Erstellen Sie spezifische Regeln in Ihrer Windows-Installation, um Dateiausführungen aus diesen Ordnern zu blockieren.

GEHEN SIE KEIN RISIKO EIN!

Die meisten Ransomware-Opfer sind schlecht darauf vorbereitet, bei einem Vorfall richtig zu reagieren. Sie verlieren daher oft kritische Daten, selbst wenn ein Lösegeld gezahlt wird. Die Folgen sind Umsatzeinbußen, verärgerten Kunden und ein beschädigtes Markenimage. Mit einigen einfache Vorsichtsmaßnahmen sowie robusten Ransomware-Gegenmaßnahmen, wie Acronis Active Protection, können Sie Ihre wertvollen Daten und Ihr Unternehmen gleichermaßen effektiv wie kosteneffizient schützen.

Weitere Informationen finden Sie unter **www.acronis.com**

Acronis