datto | BUSINESS MANAGEMENT

RMM & Patch Management:

Die erste Verteidigungslinie gegen Cyber-Bedrohungen

Cyber-Sicherheit ist eines der wichtigsten Themen in der IT-Branche. Die Verantwortung eines Managed Service Providers (MSP) für sichere IT-Umgebungen zu sorgen ist in den letzten zehn Jahren allerdings deutlich gewachsen. Der Grund: Bedrohungen treten immer häufiger auf.

Laut dem US-amerikanischen Phishing Activity Trends Report Q2-2019[1] stieg die Gesamtzahl der Phishing-Fälle vom zweiten Halbjahr 2018 bis zum ersten Halbjahr 2019 um 26 %. Der Bericht „The Human Factor 2019[2]" des US-amerikanischen IT-Unternehmens ProofPoint zeigt, dass Cyber-Kriminelle von heute weiterhin Social Engineering eMails[3] als wichtigste Angriffsstrategie nutzen. Dass die Hacker hierbei immer skrupelloser werden, zeigen die jüngsten Cyber-Angriffe der Malware GermanWiper und Ordinypt. Die Malware-Arten haben eins gemein: Einmal den Anhang geöffnet, werden nicht „nur" die Daten verschlüsselt, sondern auch überschrieben und somit unwiederbringlich unbrauchbar gemacht. Lassen sich die Unternehmen also auf die Zahlung des Lösegelds ein, verlieren sie sowohl das Lösegeld als auch die Daten.

Experten empfehlen einstimmig eine vielschichtige Security-Strategie. Dazu gehören Perimeter Hardening, Schulungen für Endnutzer, Software Patch Management und Disaster Recovery-Planung. Angriffe proaktiv zu verhindern, ist ebenfalls eine Aufgabe, die komplexer wird. Bedrohungen wie Ransomware passen sich an, wenn die präventiven Maßnahmen ausgereifter werden und neue Technologien zum Einsatz kommen. Dies macht es insbesondere kleineren Unternehmen mit begrenzten Ressourcen, schwer, den Kriminellen einen Schritt voraus zu sein.

Das Problem muss daher proaktiv gelöst werden. Das Forschungsinstitut Gartner erklärt: „Cyber-Risiken führen zu Geschäftseinbußen, Reputationsverlust, Verstößen gegen Vorschriften und Störungen im Betriebsablauf." Die Kosten von Ausfällen sind zu hoch und oft um ein Vielfaches höher als die Kosten für die Prävention. Technologie-Anbieter tragen ihren Teil dazu bei, dass Schwachstellen so schnell wie möglich behoben werden und veröffentlichen in der Regel nur wenige Stunden nach Bekanntwerden des Problems ein Update.

Eine gut dokumentierte Fallstudie ist der WannaCry-Ausbruch[4] von 2017. Microsoft erfuhr am 14. März 2017 von der Schwachstelle innerhalb des Windows-Betriebssystems und veröffentlichte am selben Tag das Sicherheitsbulletin MS17-010[5], das als CRITICAL gekennzeichnet war. Der weltweite Ausbruch ereignete sich zwei Monate später und infizierte innerhalb von 24 Stunden 230.000 Computer in 150 Ländern. Der bösartige Code, der die von Microsoft reparierte Schwachstelle ausnutzt, war fast einen Monat lang in Umlauf, bevor der Angriff stattfand. Als sich die Lage beruhigt hatte, wurde klar, dass es mindestens 300.000 Geräte gab, die das von Microsoft als kritisch gekennzeichnete Update nicht erhalten hatten.

Prominente Angriffe wie WannaCry schärfen das Bewusstsein in Unternehmen für die Risiken von Cyber-Angriffen. MSPs sollten die strategische Führung übernehmen und taktische Maßnahmen zur Sicherung der IT-Umgebungen vorschlagen. Dabei sollten sie mit Bedacht vorgehen. Beim Kunden darf kein trügerisches Sicherheitsgefühl entstehen, denn Downtime kann extrem hohe Kosten nach sich ziehen.

Erste Schritte mit Patch-Management-Services

Ein MSP hat die Möglichkeit, eine Reihe von Services anzubieten, die gebündelt oder à la carte bereitgestellt werden können.

- Analyse & Management von Schwachstellen
- Patch-Bewertungen & -Management
- Bewertung der Sicherheit der Konfiguration
- Testen der Sicherheit von Anwendungen
- Bewertung & Management der Compliance-Richtlinien

Laut Gartner ist das Ziel von Patch-Management-Services, „die Risiken von Sicherheitsverletzungen oder Performance-Problemen zu minimieren, indem die Patch-Management-Prozesse im gesamten Unternehmen standardisiert werden".

Der erste Schritt eines Services ist, die Compliance-Basis in der gesamten gemanagten Umgebung zu definieren. Bestimmen Sie dann die benötigten Mindestversionen der erforderlichen Business-Anwendungen, die installiert sein müssen. Im Anschluss identifizieren Sie die Lücken und wie diese geschlossen werden sollen. Nehmen Sie sich ausreichend Zeit, um die mit anderen Business-Anwendungen verbundenen Risiken zu verstehen und wie der Notfallplan aussieht, wenn ein Patch nicht bereitgestellt werden kann oder zu einer Störung führt.

Meistens installiert der MSP Patches in einer Sandbox- oder Test-Umgebung oder testet sie an einigen risikotoleranten Geräten. Vor dem Einsatz sollten MSPs überprüfen, ob ihre Ziele über verifizierte Backups verfügen, insbesondere, wenn es sich um Geräte handelt, die für den Betrieb von entscheidender Bedeutung sind, z. B. Server. Vergewissern Sie sich, dass alle Beteiligten die Primär- und Notfallpläne verstehen, falls das Deployment fehlschlägt. Nach der erfolgreichen Bereitstellung sollten Sie die Umgebung neu bewerten und die Konformität bestätigen. Identifizieren Sie nicht-konforme Anomalien und erstellen Sie einen Folgeplan zur Behebung. Die letzte Phase besteht darin, die Stakeholder über die Ergebnisse zu informieren.

Der Aufbau eines Services rund um das Patch Management erfordert eine Kombination aus der Dokumentation von Programmprozessen und Technologie-Toolsets. MSPs sollten ihren Kunden erläutern, dass dies eine Langzeit-Aufgabe und kein kurzfristiges Projekt ist. Alle Beteiligten sollten über Update-Frequenz, Zielgeräte sowie die Definition und Messung der Compliance informiert sein.

Die Nutzung einer vollautomatischen, richtlinienbasierten Plattform wie Datto RMM[6] ermöglicht es MSPs, Patches für typische Geschäftsanwendungen systematisch zu installieren, sobald diese verfügbar sind. Dadurch wird das Risikofenster für bekannte und Zero-Day-Schwachstellen geschlossen. Datto RMM generiert leicht verständliche Reports, die einen klaren Überblick über die Standorte und Geräte geben, die dem größten Risiko ausgesetzt sind.

Mit den entsprechenden Daten und Insights kann der MSP seine Position als strategischer Partner stärken, der proaktiv darauf achtet, Downtime zu vermeiden und die Interessen der Kunden umzusetzen.

datto

Landwehrstrasse 61
80336 München
Deutschland
Telefon: +49 (0) 89-3803 6700
www.datto.com/de
EMEApartners@datto.com

1. https://docs.apwg.org/reports/apwg_trends_report_q2_2019.pdf
2. https://www.proofpoint.com/sites/default/files/gtd-pfpt-au-r-human-factor-2019.pdf
3. https://www.datto.com/blog/5-types-of-social-engineering-attacks
4. https://www.datto.com/blog/why-are-ransomware-attacks-like-wannacry-so-effective
5. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010
6. https://www.datto.com/de/business-management/datto-rmm