Wenn aus Daten Geiseln werden: Vier Schritte für einen effektiven Schutz vor Ransomware

29.05.2017, 14:52 | IT, New Media & Software

Pressemitteilung von: *DeskCenter Solutions AG*
Presseagentur: *campaignery*

Christoph A. Harvey, Vorstandssprecher, DeskCenter Solutions AG

DeskCenters Cyber Security Lösungen mit über 1000 Kunden schließen bereits seit 10 Jahren zuverlässig Einfallstore für Hacker

Leipzig, 29. Mai 2017 – Der Cyber-Angriff durch den Krypto-Trojaner WannaCry belegt, dass nur ein zuverlässiges und

vor allem zeitnahes Patch- und Versionsmanagement die Sicherheit der IT-Infrastruktur gewährleistet. Der Software-Hersteller DeskCenter Solutions AG warnt in diesem Zusammenhang eindringlich vor Quick Fixes: Unternehmen sollten jetzt nicht nur kurzfristige Maßnahmen zum Schutz vor dem WannaCry-Trojaner ergreifen, mahnt Christoph A. Harvey, Chief Excecutive Officer bei DeskCenter. Wesentlich effektiver, weil nachhaltiger, sei es, einen ganzheitlichen Schutz vor Ransomware zu etablieren, so Harvey. Sein Unternehmen, seit 10 Jahren mit entsprechenden Lösungen am Markt, hat hierzu unter http://www.deskcenter.com/de/intern/downloadsnavi/whitepapers/ einen Vier-Stufen-Check zum Download herausgegeben. Damit können IT-Verantwortliche systematisch prüfen, wie gut sie bereits vor Ransomware-Befall geschützt sind und welche Maßnahmen sie noch zusätzlich ergreifen sollten.

Über 220.000 Systeme wurden vorletzte Woche vom Verschlüsselungstrojaner WannaCry befallen. Und das obwohl Microsoft bereits am 14. März 2017 einen Patch für diese Sicherheitslücke bereitgestellt hatte. Dass so viele Systeme dennoch nicht rechtzeitig gepatcht wurden, beweist, dass die Sicherheits- und IT-Prozesse in vielen Unternehmen noch unzureichend unterstützt sind. Unternehmen sollten WannaCry zum Anlass nehmen, die Absicherung ihrer gesamten IT-Infrastruktur zu prüfen und mit Cyber Security Lösungen zu stützen.

„Die weltweite Verbreitung dieses Trojaners hat viele Unternehmen aufgeschreckt. Kurzfristig versuchen diverse Hersteller mit Test- oder Gratisversionen bei Unternehmen zu punkten. Für eine nachhaltige Prävention reicht dies jedoch nicht aus“, so Christoph A. Harvey. „Um sich künftig vor ähnlichen Angriffen zu schützen, müssen Unternehmen alle Geräte und Anwendungen in ihrem Netzwerk ständig genau kennen. Sie müssen außerdem sämtliche Software – nicht nur Windows – immer aktuell halten.“

Um dies zu gewährleisten, ist ein Bündel an Maßnahmen nötig. DeskCenter empfiehlt Unternehmen

* ... regelmäßig zu überwachen, welche Programme auf Firmengeräten installiert sind – einschließlich „potenziell riskanter Installationen“ wie beispielsweise Adware, Toolbars, portable Apps oder Spiele.
* ... laufend den Stand der Programme zu prüfen: Denn die Sicherheit hängt maßgeblich davon ab, ob Software-Versionen aktuell oder veraltet sind oder ob sie vom Hersteller sogar schon abgekündigt wurden.
* ... Lücken zeitnah zu schließen und das Patching zu automatisieren.
* ... die Zugriffsrechte der Mitarbeiter auf Dateien und Ordner zu prüfen und über Access Management die Auswirkungen einer Ransomware-Attacke einzudämmen.

Mit dieser letzten Maßnahme betreiben Unternehmen aktive Schadensbegrenzung für den Fall, der hoffentlich niemals eintritt: Nämlich, dass Hacker eine neue Schwachstelle ausnutzen, für die der Softwareanbieter noch keinen Patch herausgegeben hat. „Fake-E-Mails mit schadhaften Links sind heute von ‚echten‘ E-Mails kaum mehr zu unterscheiden. Die Wahrscheinlichkeit, dass ein Mitarbeiter versehentlich auf einen schadhaften Link klickt, steigt damit massiv. Dann gilt es den Schaden, der durch die Verschlüsselung entsteht, weitestgehend einzugrenzen“, erklärt Harvey.

Basierend auf der über zehnjährigen Erfahrung im Software Asset Management hat DeskCenter für die Abwehr von Ransomware alle relevanten Funktionen der DeskCenter Management Suite zu zwei Cyber Security Lösungen gebundelt: Zum einen in der DeskCenter Windows Security, die eine vollständige Inventarisierung für Microsoft Windows Betriebssysteme und Microsoft Anwendungen, sowie eine automatische Verteilung und Installation von allen Patches ermöglicht. Zum anderen in eine Lösung für die gesamte IT-Infrastrukur, die DeskCenter Premium Security. Diese erkennt neben Windows sämtliche installierte Anwendungen und Hilfsprogramme auf allen Geräten im Netzwerk. Dazu gleicht sie die gefundenen Applikationen mit einem Katalog an Programmen von über 14.000 Herstellern ab. Ein Patchlevel Security Dashboard zeigt tagesaktuell potenzielle Sicherheitsrisiken auf und ermöglicht den direkten Roll-out fertig paketierter, aktueller Patches und Updates. Zudem lassen sich unerwünschte und veraltete Software direkt löschen. Ebenfalls enthalten ist ein Access Management für Dateien und Ordner. Weitere Informationen zu den Security-Lösungen von DeskCenter finden sich in dem Whitepaper „Wenn aus Daten Geiseln werden: Vier Schritte für einen effektiven Schutz vor Ransomware“ (http://www.deskcenter.com/de/intern/downloadsnavi/whitepapers).

Portrait

Über die DeskCenter Solutions AG
Die DeskCenter® Solutions AG ist ein international agierender, deutscher Softwarehersteller mit Sitz in Leipzig. Ihre technologisch führenden Lösungen für Unternehmen, öffentliche Organisationen und Cloud Service Provider bilden den gesamten IT Management Prozess ab. Hierzu gehören neben Assetmanagement, Lizenzmanagement, Softwareverteilung und OS Deployment auch ein leistungsfähiges Reporting, ein Service-Desk-Modul, Mobile Device Management und ein umfangreiches Realtime System Management. Alle Module sind ganzheitlich entwickelt, lassen sich aber auch einzeln einsetzen.

1.200 namhafte Kunden vertrauen auf die mehrfach preisgekrönte Software des 2007 gegründeten Unternehmens: darunter Engelbert Strauss, HEITEC, Kraft Foods, Lufthansa AirPlus, Sonax, oder Volkswagen.

Die Kunden von DeskCenter schätzen insbesondere den schnellen und kompetenten Support sowie die aktive Einbindung bei der Weiterentwicklung. Für eine optimale Betreuung der Kunden ist das Unternehmen weltweit durch ein leistungsfähiges Partnernetzwerk vertreten. Systemhäuser und Systemintegratoren, die innovative Managed Services anbieten, profitieren von einem attraktiven Partnerprogramm.

deskcenter.com

News-ID: 952876 • Views: 622 (Stand: 03.06.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/952876/Wenn-aus-Daten-Geiseln-werden-Vier-Schritte-fuer-einen-effektiven-Schutz-vor-Ransomware.html