StorageCraft Studie zeigt Bedarf für Ransomware-Realitätscheck auf

CORK/MÜNCHEN – 12. Dezember 2019 – StorageCraft®, das sich den Schutz von Daten und deren ständige Verfügbarkeit zum Ziel gesetzt hat, gab heute weitere Ergebnisse einer unabhängigen weltweiten Forschungsstudie bekannt. Im Rahmen der Studie wurden die IT-Entscheidungsträger von mehr als 700 Unternehmen in Australien, Frankreich, Deutschland, Nordamerika und Großbritannien zum Thema Datenmanagement befragt. Die Ergebnisse verdeutlichen die klaffende Lücke zwischen der Zuversicht von Unternehmen, sich von einem Ransomware-Angriff erholen zu können, und deren tatsächlicher Fähigkeit, Daten wiederherstellen zu können. Zwar geben 68 Prozent der Befragten (Deutschland: 72 Prozent) an, einen klaren Plan zu haben und sich schnell von einem Ransomware-Angriff erholen zu können. Allerdings testet ein knappes Viertel, 23 Prozent, (Deutschland: 23 Prozent) die vorhandenen Pläne zur Systemwiederherstellung nicht einmal. Knapp die Hälfte, 46 Prozent (Deutschland: 44 Prozent), derjenigen, die überhaupt derartige Tests durchführen, tut dies nur einmal pro Jahr oder seltener.

Was die Erholungsfähigkeit nach einem Ransomware-Angriff angeht gibt es einen weiteren Indikator, der die Kluft zwischen Wahrnehmung und Realität bestätigt. So gaben die meisten Befragten, 86 Prozent (Deutschland: 90 Prozent), an, bereits einmal einen Datenverlust erlitten zu haben. Über ein Viertel, 27 Prozent (Deutschland: 26 Prozent), machten diese Erfahrung sogar erst kürzlich: in den letzten sechs Monaten. Die Studie entlarvt auch beim Budget und der Komplexität der IT-Infrastruktur versteckte Probleme, sodass die Vorbereitung auf potenzielle Ransomware-Angriffe noch anspruchsvoller wird.

StorageCraft Technology Corporation
380 Data Drive, Suite 300, Draper, Utah 84020 USA
P 801.545.4700 F 801.545.4705

- Knapp die Hälfte der Befragten, 46 Prozent (Deutschland: 41 Prozent), erklärte, nicht über das nötige Budget für ein angemessenes Datenmanagement und die entsprechenden Wiederherstellungsmöglichkeiten nach einem Ausfall zu verfügen.
- Ebenso gab knapp die Hälfte der Befragten, 49 Prozent (Deutschland: 46 Prozent), an, drei bis fünf verschiedene Arten von Datenmanagement- und Datenschutzsystemen im Einsatz zu haben. Ein Drittel, 33 Prozent (Deutschland: 53 Prozent), verfügen gar über sechs oder mehr verschiedene Systemtypen, die im Falle eines Datenverlustes koordiniert und wiederhergestellt werden müssen.

Shridar Subramanian, Vice President Marketing und Produkt Management bei StorageCraft sagt dazu: „Obwohl Unternehmen immer wieder Opfer von Ransomware werden – allein im ersten Quartal dieses Jahres stiegen die gemeldeten Vorfälle[1] um 118% – zeigen unsere Untersuchungen, dass immer noch zu viele Organisationen nur über einen unzureichenden Datenschutz verfügen. Unternehmen müssen dringend einen Realitätscheck durchführen und dabei bewerten und testen, wie effektiv ihre Schutzmaßnahmen gegen Ransomware-Angriffe tatsächlich sind und wie gut sie sich von diesen Attacken erholen können."

StorageCraft empfiehlt Unternehmen, alle Pläne für Angriffsprävention, Störungsbehebung und Wiederherstellung regelmäßig zu überprüfen und zu testen. Zuerst sollten Unternehmen dabei ihre geschäftskritischen Daten ermitteln und lokalisieren, sowie umfangreiche Schutzmaßnahmen einleiten. Dieser Schritt umfasst E-Mail-Sicherheitssysteme, Firewalls, regelmäßige

[1] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf

Software-Updates, eindeutig überprüfbare Verwaltungs- und Zugriffsrichtlinien, sowie eine kontinuierliche Schulung der Anwender.

Prävention bietet allerdings keinen vollständigen Schutz. Deshalb ist ein konkreter Plan zur Störungsbehebung und Wiederherstellung im Fall von Ransomware-Angriffen von entscheidender Bedeutung. Die Vereitelung solcher Angriffe ist abhängig davon, wo die Daten gespeichert werden (also am Standort, in der Cloud oder in cloudbasierten Anwendungen, wie beispielsweise G Suite oder Office 365) und welchen Wiederherstellungsort das Unternehmen bevorzugt. Entscheidende Elemente eines erfolgreichen Plans zur Ransomware-Behebung und der anschließenden Wiederherstellung sind unter anderem:

Unveränderbare Momentaufnahmen: Um die Wiederherstellung unstrukturierter Daten zu ermöglichen, sollten Unternehmen ihre Informationen mittels laufender unveränderbarer Momentaufnahmen schützen. Auf diese Weise erfasste Daten werden „eingefroren“ und lassen sich von Ransomware-Angreifern nicht überschreiben oder löschen. So kann das Unternehmen jederzeit und in kürzester Zeit seine Systeme auf einen sicheren Datensatz zurücksetzen.

Orchestrierung: Ein erfolgreicher Wiederherstellungsprozess erfordert die Priorisierung geschäftskritischer Daten und Anwendungen. Unternehmen, die eine cloudbasierte Wiederherstellung nutzen, sollten vorab die Reihenfolge festlegen, in der Daten und Anwendungen wiederhergestellt werden. Diese „Orchestrierung“ sorgt für minimale Ausfallzeiten während der Datenwiederherstellung.

Sofortige Wiederherstellung: Laut Branchenanalyst Gartner[2] kostet eine Minute Ausfall bis zu 5.600 US-Dollar. Vor diesem Hintergrund wird deutlich, wie wichtig der Faktor Geschwindigkeit im Störungsbehebungs- und Wiederherstellungsprozess nach einem Ransomware-Angriff ist. Lösungen wie StorageCraft VirtualBoot ermöglichen die sofortige Wiederherstellung virtueller und physischer Infrastrukturen – sowie strukturierter und unstrukturierter Daten.

Failback: Nach einer erfolgreichen cloudbasierten Wiederherstellung besteht der letzte Schritt der Behebung einer Ransomware-Infektion darin, die Dateninfrastruktur an ihren ursprünglichen Ort zurückzuverlagern und den gewohnten Betrieb wieder aufzunehmen. Der geplante Failback-Prozess sollte sich möglichst wenig auf Produktionsanwendungen auswirken, um zusätzliche Ausfallzeiten und eine Geschäftsbeeinträchtigung zu minimieren.

Folgen Sie StorageCraft auch auf Twitter, LinkedIn und Facebook.
Aktuelle Artikel zum Thema Datensicherung und Wiederherstellung sind im StorageCraft Blog zu finden.

###

Über StorageCraft
Mit den Lösungen von StorageCraft für Datensicherung, Datenmanagement und Business Continuity halten Unternehmen ihre kritischen Informationen stets sicher, zugänglich und optimiert. Die leistungsstarken Angebote für Datensicherheit von StorageCraft bieten sofortige, zuverlässige und vollständige Datenwiederherstellung und eliminieren Ausfallzeiten. Die

[2] https://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/

innovative und konvergente Scale-out-Plattform für Primär- und Sekundärspeicher mit integrierter Datensicherung löst die Herausforderungen des Datenwachstums. Sie ist effizient und einfach in der Anwendung für lokale, Cloud-basierte oder hybride Umgebungen. Weitere Informationen finden Sie unter StorageCraft.com.

Unternehmenskontakt

Jock Breitwieser
StorageCraft Technology Corp.
+1 408.800.5625
jock.breitwieser@storagecraft.com

Agenturkontakt

TC Communications
Arno Lücht
+49 8081 9546-19
Thilo Christ
+49 8081 9546-17
storagecraft@tc-communications.de
www.tc-communications.de