Vier Technologien für den Schutz vor Ransomware-Angriffen

von Naveen Chhabra

18. Oktober 2019

Warum Sie diesen Bericht lesen sollten

Als Verantwortliche für die Wiederherstellung nach Ausfällen haben die Zuständigen für Infrastruktur und Betrieb (I&O) erfolgreich Wiederherstellungen in allen möglichen Situationen durchgeführt, außer in einer: nach Ransomware-Angriffen. Ransomware-Angriffe führen nicht zu einer bekannten Art Ausfall, sondern belasten oft die Backup-Infrastruktur an sich. Es geht dabei nicht nur um die Wiederherstellung nach einem Backup. I&O-Experten müssen eng mit ihren Sicherheits- und Risiko-Kollegen (S&R) zusammenarbeiten, um sicherzustellen, dass sie die Wiederherstellung mit einer nicht infizierten Kopie ausführen. Gemeinsam können sie vier Technologien einsetzen, um die Widerstandsfähigkeit gegenüber Ransomware zu verbessern.

Die wichtigsten Schlussfolgerungen

Mangelnde Transparenz bereitet I&O-Profis Sorgen

I&O-Experten verfügen über Tools und Technologien, mit denen sie schnell von jeder Backup-Instanz Wiederherstellungen durchführen können. Sie haben jedoch keine Möglichkeit, die neueste Backup-Kopie zu identifizieren, die auch noch nicht infiziert ist.

Fügen Sie Ihrem Arsenal vier Technologien hinzu, um Vertrauen und Wiederherstellbarkeit zu verbessern

I&O-Experten müssen proaktive Strategien anwenden und vier Technologien kombinieren: WORM-Speicher, Lösungen zur Ausfallsicherheit von Daten, unveränderliche Dateisysteme und Multifaktor-Authentifizierung. Diese Technologien sind nicht neu. I&O-Experten nutzen sie, um eine Vielzahl von Geschäftsanforderungen zu erfüllen. Setzen Sie diese Technologien ein, um nach Ransomware-Angriffen wieder Vertrauen zu fassen und die Wiederherstellbarkeit zu verbessern.

Vier Technologien für den Schutz vor Ransomware-Angriffen

von Naveen Chhabra
mit Beiträgen von Glenn O'Donnell, Amanda Lipson und Bill Nagel
18. Oktober 2019

Ransomware-Angriff: Ein Reality-Check, der proaktive Prävention erfordert

Ransomware paralysiert weiterhin öffentliche und private Unternehmen weltweit.[1] Das Weltwirtschaftsforum zählt Cyberangriffe zu den Top 10 der globalen Risiken in Bezug auf das Auftreten und die Auswirkungen, doch Unternehmen werden oft unvorbereitet getroffen.[2] Nach einem Angriff verlangen Führungskräfte vom I&O-Team, Daten mithilfe von Backup- oder Archivkopien wiederherzustellen.[3] Strafverfolgungsbehörden raten Unternehmen von der Zahlung von Lösegeldern ab. Stattdessen empfehlen sie, in Prävention und verbesserte Wiederherstellbarkeit zu investieren.[4] Sicherungen sind wichtig, reichen jedoch nicht aus. Ransomware verursacht Kollateralschäden, indem sie neben Ihrer letzten Verteidigungslinie, der Backup-Infrastruktur, auch die Produktionssysteme angreift. Seit ihrer Erfindung vor drei Jahrzehnten haben sich Ransomware-Angriffe stetig weiterentwickelt:

- **Sie sind zielgerichteter geworden, um einen maximalen Gewinn zu erzielen – für die Kriminellen.** Cyberkriminelle kehren immer häufiger Massenangriffen den Rücken und führen gezielte Ransomware-Angriffe durch. Aktuelle Beispiele zeigen, dass Angreifer nicht nur einfache Ziele ins Visier nehmen. Im vergangenen Jahr haben Angriffe auf Stadtverwaltungen und bundesstaatliche Behörden erheblich zugenommen.[5] Angreifer nutzen oft außer Acht gelassene Schwachstellen, um in die Umgebung eines Opfers einzudringen. Die treibende Kraft hinter dieser neuen Herangehensweise ist die Rendite: Ein erfolgreicher Angriff auf ein bestimmtes Unternehmen oder eine Schwachstelle kann viel lukrativer sein als ein generalisierter Angriff.
- **Sie sind deutlich stärker, häufiger, anspruchsvoller und intensiver geworden.** In den letzten Jahren haben Unternehmen eine deutliche Zunahme der Ransomware-Angriffe beobachtet. Angreifer nutzen ausgeklügelte Technologien und werden bei jedem Angriff präziser, was für die Opfer wesentlich härtere Folgen hat. Eine Arztpraxis in Michigan beschloss nach einem Angriff, zu schließen.[6]

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

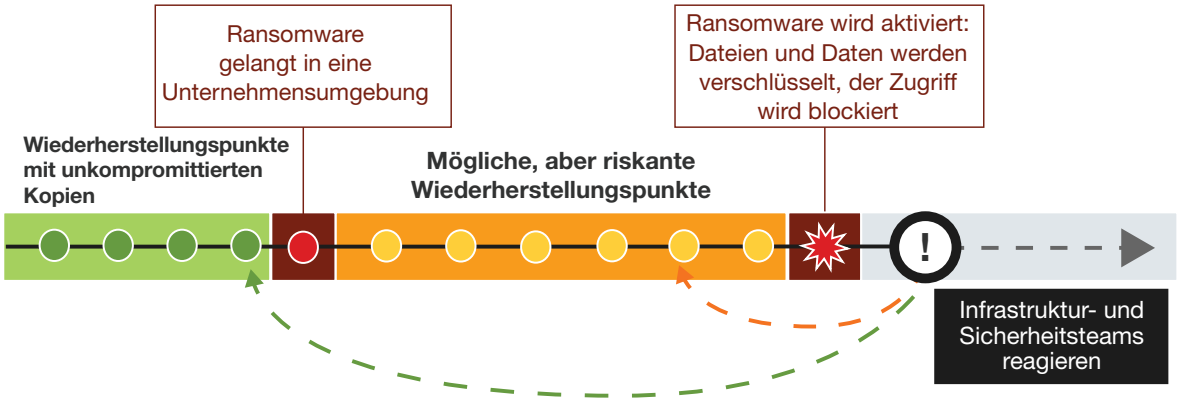
Herausforderungen: Transparenz der Wiederherstellung und Vertrauen

Unternehmen befinden sich auf dem Weg zur digitalen Transformation. Bei der digitalen Transformation werden Anwendungen zusammengeführt, die Kunden rund um die Uhr eine bessere Serviceerfahrung in Form von einheitlichen Geschäftsprozesses bieten sollen. Eine engere Integration kann jedoch dazu führen, dass Anwendungen anfälliger werden, da jede noch nicht behobene Schwachstelle zu einer Achillesferse des Unternehmens werden und den Service unterbrechen kann. Ransomware-Angriffe verursachen Ausfälle, die sich hinsichtlich Wiederherstellungsplänen, Verfügbarkeit von Daten und Infrastruktur, teamübergreifender Zusammenarbeit und dem Risiko, Daten nicht wiederherstellen zu können, stark unterscheiden. Kritisch ist, dass IT-Führungskräfte keine Möglichkeit haben, die Wiederherstellbarkeit unabhängig zu messen, was die Transparenz des Wiederherstellungszustands einschränkt und das Vertrauen in die Wiederherstellbarkeit beeinträchtigt.[7] Die Geschäftsverluste durch Ausfälle zeigen immer wieder, dass IT-Führungskräfte mehr in Ausfallsicherheit investieren müssen, da die Verluste durch einen Angriff weit über die Ausgaben hinausgehen, die zur Verbesserung der Ausfallsicherheit erforderlich sind.[8]

- **Ransomware dringt in IT-Umgebungen ein und bleibt dort.** Malware gelangt auf unauffällige Weise in die IT-Infrastruktur des Unternehmens. Sobald sie einmal drin sind, wollen Angreifer ihre Auswirkungen maximieren, indem sie so viele Systeme wie möglich infizieren. Dazu infiltriert Malware langsam die Umgebung. Sie bleibt im Tarnmodus, sodass sie nicht bemerkt wird. Ransomware ruht in der Regel Wochen oder Monate lang in einer Umgebung und bleibt für Sicherheitsteams normalerweise unsichtbar (siehe Abbildung 1).[9] Berichten zufolge entdeckte das Infrastruktursicherheitsteam von Bayer vor mehr als einem Jahr Malware in seiner IT-Umgebung. Die Malware wurde nicht aktiviert, und Bayer überwachte ihre Bewegungen kontinuierlich.[10] Aber nur wenige Unternehmen können Ransomware-Infektionen und -Bewegungen erfolgreich erkennen, was den I&O-Profis Sorgen bereitet. Da sie nicht wissen, wann und wie die Umgebung infiziert wurde, ist ihre Fähigkeit, nicht infizierte Daten erfolgreich wiederherzustellen, deutlich eingeschränkt.

- **IT-Führungskräfte müssen einen deterministischen, nicht wahrscheinlichkeitsbasierten Ansatz verfolgen.** Die Backup-Infrastruktur ist die letzte und beste Verteidigungslinie gegen Ransomware-Angriffe. Aufgrund ihrer ruhenden Eigenschaften ist es fast sicher, dass die Malware auch Sicherungskopien infizierter Systeme infiziert hat. Erfolgt die Wiederherstellung mithilfe einer infizierten Kopie, erhält Ransomware erneut die Kontrolle über die Systeme. I&O-Experten verwenden in der Regel einen mühsamen Trial-and-Error-Ansatz, indem sie jede vorangegangene Sicherungskopie wiederherstellen und auf Infektionen und andere Schwachstellen testen. Der Vorgang wird fortgesetzt, bis die letzte unkompromittierte Backup-Kopie gefunden wurde. Dieser probabilistische Ansatz ist unpraktisch, da die I&O-Teams nicht über die Zeit und Hardware verfügen, um endlose Versuche zu bewältigen. Um Wiederherstellungsmaßnahmen zu unterstützen, müssen S&R-Teams Ransomware-Infektionen aufspüren. I&O- und S&R-Teams müssen gemeinsam die neueste nicht infizierte Backup-Instanz mit einem deterministischen Ansatz finden. Während dieser Ansatz Stakeholdern sympathisch erscheint, weil er die Wiederherstellungsvorgänge effektiver gestaltet, haben nur sehr wenige Unternehmen eine Partnerschaft zwischen ihren I&O- und S&R-Teams aufgebaut.[11]

ABBILDUNG 1: Anatomie eines Ransomware-Angriffs



Vier Technologien erhöhen die Transparenz und das Vertrauen

Unternehmen müssen ihr strategisches Denken ändern, um eine steigende Anzahl von Cyberbedrohungen bewältigen zu können. Sie können das Lösegeld zahlen, Geschäftsdaten und Transaktionen verlieren, während I&O-Profis sich bemühen, Wiederherstellungen von Punkten auszuführen, die möglicherweise nicht aktuell sind, oder in die Stärkung der Sicherheits- und Wiederherstellungsfähigkeiten investieren. Unternehmen, die sich für die Zahlung des Lösegelds entscheiden, müssen überlegen, ob die Täter alle Daten wiederherstellen werden. Vielleicht nehmen sie sich auch einen Nachschlag. Cyberkriminelle greifen zahlende Opfer sehr wahrscheinlich erneut an, und Sie haben keine Gewissheit, dass sie keine Malware zurücklassen.[12] Unternehmen, die ältere Wiederherstellungspunkte nutzen, können erhebliche Mengen an Geschäftstransaktionen verlieren – ein Datenverlust, der ein erhebliches finanzielles und rechtliches Haftungsrisiko darstellt. Die Entscheidung, in effektiven Schutz zu investieren, hängt von der aktuellen Sicherheitslage und Risikobereitschaft Ihres Unternehmens ab. I&O-Profis haben nur wenige Möglichkeiten, Ransomware-Angriffe zu erkennen, Systeme vor ihnen zu schützen und Daten nach Angriffen schnell und zuverlässig wiederherzustellen.

Nutzen Sie bekannte Technologien zur Verbesserung von Erkennung, Fehlerbehebung, Schutz und Wiederherstellung

Vorbeugen ist besser als heilen. Jede Ebene einer Unternehmensinfrastruktur weist Schwachstellen auf.[13] Trotz der Vielzahl an verfügbaren Sicherheitstools und menschlicher Kompetenzen haben Unternehmen bei der Erkennung von Ransomware große Schwierigkeiten. Unternehmen sollten Infrastrukturfunktionen – Plattform, Hardware oder Software – erweitern, um die Wahrscheinlichkeit für eine Malware-Erkennung, den Schutz davor und die Wiederherstellungsfähigkeit zu erhöhen. Ebenso müssen sie die Zusammenarbeit zwischen den I&O- und S&R-Teams ermöglichen, damit diese in Krisensituationen zusammenarbeiten können. Um ihre Fähigkeiten zu verbessern, können I&O-Profis die folgenden Technologien nutzen:

› **WORM-Speicher gewährleistet, dass Daten nicht beschädigt werden können.** I&O-Experten verwenden schon seit langem WORM-Speicher, um Datenarchive zu sichern und unveränderlich zu gestalten. WORM-Speicher sperrt Daten zur Aufbewahrung. d. h. Daten können nur einmal geschrieben und danach nicht mehr geändert werden. Ein neuer Schreibvorgang schreibt neue Daten in nicht verwendete Speicherblöcke.

WORM-Speicher erfüllt gesetzliche Compliance-Anforderungen wie SEC Rule 17a-4, HIPAA und PCI-DSS.[14] Anbieter von lokalen Speicherlösungen wie IBM und NetApp sowie Anbieter von Public-Cloud-Speicherlösungen wie Amazon Web Services, Google Cloud und Microsoft Azure bieten diese Speicherklasse an. Wenn Sie Sicherungskopien geschäftskritischer Anwendungen in WORM-Speicher ablegen, werden diese vor betrügerischen Änderungen bewahrt, sodass Sie sicher sein können, dass nicht infizierte Kopien von Daten wiederhergestellt werden.

- **Ein unveränderliches Dateisystem arbeitet Hand in Hand mit WORM-Speicher.** Durch die Implementierung eines unveränderlichen Dateisystems mit zugrunde liegendem WORM-Speicher wird das System aus der Perspektive des Ransomware-Schutzes wasserdicht. Sie können dies jedoch nicht für die Gesamtheit aller Daten aus Geschäftsanwendungen implementieren, da ansonsten Ihr Bedarf an Speicherkapazität unkontrollierbar wächst. Je nach Anwendung und Datenrisikoprofil speichern Sie Backup-Daten mit spezifischen Aufbewahrungsanforderungen mit festgelegter Häufigkeit in einem unveränderlichen Dateisystem, gefolgt von inkrementellen Backups auf herkömmlichem Speicher. Ein sorgfältiges Design mit unveränderlichen Systemen erhöht die Ausfallsicherheit der Daten.
- **Datenresilienz-Tools, die Anomalien erkennen, lösen proaktive Benachrichtigungen aus.** Moderne Datenresilienz-Tools können Sicherungskopien untersuchen, um mögliche Ransomware-Aktionen und -Infektionen zu erkennen.[15] Typische Ransomware-Angriffe umfassen Aktionen wie das Verschlüsseln oder Löschen von Datendateien, das Ändern von Dateierweiterungen oder das Ändern von Dateien auf eine Weise, die nicht mit den normalen Aktivitäten eines Benutzers oder einer Anwendung vereinbar ist. Ohne proaktive Analyse durch Datenresilienz-Tools bleiben diese Aktionen unentdeckt. Diese Tools können Sicherungsdaten auf solche Aktivitäten überwachen und das IT- oder Sicherheitspersonal benachrichtigen. Der Nachteil besteht darin, dass diese Tools auch Fehlalarme auslösen können – wobei Fehlalarme immer noch besser sind als gar keine Erkennung.
- **Eine Multifaktor- oder Multipersonen-Authentifizierung gewährleistet, dass unbefugte Aktionen blockiert werden.** Die Multifaktor-Authentifizierung ist eine effektive, proaktive Methode, um Probleme im Identitäts- und Zugriffsmanagement zu lösen, die Sicherheit zu verstärken und Datenkonsistenz, Zuverlässigkeit und Verfügbarkeit zu erhalten. I&O-Experten können Multifaktor- und Multipersonen-Authentifizierung einführen, um sicherzustellen, dass Sicherungen nicht kompromittiert werden, und um die Kontrolle über kritische Aufgaben im Zusammenhang mit geschützten Daten zu stärken. So können Angreifer selbst mit gestohlenen Admin-Berechtigungen keine Backups löschen.

Empfehlungen

Fördern Sie eine enge Partnerschaft zwischen I&O und S&R, um Ransomware zu bekämpfen

Der Schutz des Unternehmens vor Ransomware liegt in der gemeinsamen Verantwortung von Experten für I&O und S&R. Die Arbeit in Silos hat jedoch die Fähigkeit von Unternehmen, mit diesen Angriffen umzugehen, bedeutend geschwächt. Teamübergreifende Zusammenarbeit ist eine der wichtigsten Voraussetzungen für die effektive und effiziente Bewältigung von Ausfällen, die durch Ransomware-Angriffe verursacht werden. Einige der empfohlenen Technologien, wie WORM-Speicher und ein unveränderliches Dateisystem, liegen direkt im Verantwortungsbereich von I&O; andere, wie z. B. die Multifaktor-Authentifizierung, sind mehr in S&R angesiedelt. Es besteht jedoch zunehmend die Notwendigkeit, dass diese beiden Bereiche gemeinsam Probleme lösen, indem sie:

› **Herausfinden, wie sie am besten zusammenarbeiten, um die Sicherheit zu stärken.** I&O-Experten kennen sich bezüglich Datenausfallsicherheit sehr gut aus. Es ist an der Zeit, Möglichkeiten für die Zusammenarbeit mit S&R zu erkennen und das Know-how beider Seiten zu nutzen, um die Sicherheit zu verbessern. Bedenken Sie Folgendes: I&O-Experten können WORM-Speicher bereitstellen, benötigen jedoch das Fachwissen von S&R, um Multifaktor-Authentifizierungskontrollen einzurichten. Ohne Multifaktor-Authentifizierung kann weiterhin auch unbefugt auf WORM-Speicher zugegriffen werden.

› **Einen gemeinsamen Wiederherstellungsplan für Ransomware-Angriffe entwickeln.** Die Wiederherstellung nach durch Ransomware verursachten Ausfällen ist eine gemeinsame Verantwortung, die verschiedene Perspektiven kombiniert: die Identifizierung einer unkompromittierten, nicht infizierten Sicherungskopie, die Definition einer Wiederherstellungsinfrastruktur, eines Prozesses und eines Plans, die Bewertung der Sicherheit bei der Wiederherstellung von Instanzen und die Sicherstellung, dass nach der Wiederherstellung keine bestehenden oder neuen Schwachstellen verbleiben. Die I&O- und S&R-Teams müssen sich auf einen Wiederherstellungsplan einigen, den beide Teams verfolgen können.

Zusätzliches Material

Unternehmen, die für diesen Bericht befragt wurden

Wir möchten uns bei den Mitarbeitern der folgenden Unternehmen bedanken, die sich während der Studie großzügig Zeit für diesen Bericht genommen haben.

Cohesity

CommVault

Rubrik

Spin.ai

Fußnoten

[1] Der erste Ransomware-Angriff wurde 1989 erkannt; jahrzehntelang nahm die Anzahl bekannter Ransomware-Angriffe nicht stark zu. Seit 2016 treten diese Angriffe jedoch viel häufiger auf und haben in ihrer Intensität, Häufigkeit und Wirkung zugenommen.

Quelle: „Ransomware“, KnowBe4 (https://www.knowbe4.com/ransomware).

[2] Quelle: „The Global Risks Report 2019: 14th Edition“ (Weltweiter Risikobericht 2019: 14. Ausgabe), Weltwirtschaftsforum, Januar 2019 (http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf).

Obwohl Befragte angaben, dass sie bei Ransomware-Angriffen sicher eine Wiederherstellung durchführen können, rechtfertigten ihre Teamorganisation, Mitarbeiter und Prozesse dieses Vertrauen nicht. Vorfälle in der Branche lassen ebenfalls andere Schlüsse zu. Lesen Sie den Forrester-Bericht „Ransomware Is A Business Continuity Issue“ (Ransomware ist ein Problem der Geschäftskontinuität).

[3] Norsk Hydro hat alle IT-Systeme für den Anlagenbetrieb während eines Ransomware-Angriffs verloren. Die Geschäftsleitung erklärte, dass sie kein Lösegeld zahlen würde, sondern sich auf ihre Backup-Systeme zur Wiederherstellung verlassen würde. Quelle: Eduard Kovacs, „Norsk Hydro Restoring Systems, But Not Paying Ransom“ (Norsk Hydro stellt Systeme wieder her, zahlt jedoch kein Lösegeld), Security Week, 20. März 2019 (https://www.securityweek.com/norsk-hydro-restoring-systems-not-paying-ransom).

[4] Das US Federal Bureau of Investigation hindert Unternehmen, die Ransomware-Angriffen ausgesetzt sind, daran, das Lösegeld zu zahlen. Quelle: Josephine Wolff, „They Stole Your Files, You Don't Have to Pay the Ransom“ (Sie haben Ihre Dateien gestohlen, Sie müssen kein Lösegeld bezahlen), The New York Times, 14. August 2019 (https://www.nytimes.com/2019/08/14/opinion/ransomware.html).

[5] Quelle: Kara Frederick, „The Rise of Municipal Ransomware“ (Zunehmendes Auftreten von Ransomware in Gemeindeverwaltungen), City Journal, 3. September 2019 (https://www.city-journal.org/ransomware-attacks-against-cities).

[6] Quelle: Marianne Kolbasuk McGee, „Medical Practice to Close in Wake of Ransomware-Attack“ (Arztpraxis schließt nach Ransomware-Angriff), Bank Info Security, 2. April 2019 (https://www.bankinfosecurity.com/medical-practice-to-close-in-wake-ransomware-attack-a-12321).

[7] Lesen Sie den Forrester-Bericht „The State Of Business Technology Resiliency, Q2 2017“ (Zustand der Ausfallsicherheit der Geschäftstechnologie, 2. Quartal 2017).

[8] Große Fluggesellschaften haben durch Ausfälle Millionen von Dollar verloren.

Quelle: Naveen Chhabra, „Lessons Learned From The Recent British Airways Outage“ (Lehren aus dem kürzlichen Ausfall bei British Airways), Forrester Blogs, 15. Juni 2017 (https://go.forrester.com/blogs/17-06-15-lessons_learned_from_the_recent_british_airways_outage/).

Quelle: Leslie Josephs, „Delta: Atlanta power failure cost it up to $50 million.html“ (Delta: Stromausfall in Atlanta verursacht Kosten bis zu 50 Mio. USD), CNBC, 3. Januar 2018 (https://www.cnbc.com/2018/01/03/delta-atlanta-power-outage-cost-it-up-to-50-million.html).

[9] Bayer erkannte ansteckende Software in seiner IT-Infrastruktur und verfolgte ihre Bewegungen, Aktionen und Interessen, bevor sie aus den Systemen entfernt wurde. Bayer konnte zwar seine Ransomware erkennen, doch nicht alle Unternehmen verfügen über diese Reife und Fähigkeit. Quelle: Phil Taylor, „Bayer hit by extensive, year-long cyber-attack“ (Bayer von umfassender, jahrelanger Cyber-Attacke getroffen), Securing Industry, 5. April 2019 (https://www.securingindustry.com/pharmaceuticals/bayer-hit-by-extensive-year-long-cyber-attack/s40/a9646/).

[10] Quelle: Patricia Weiss und Ludwig Burger, „Bayer contains cyber attack it says bore Chinese hallmarks“ (Bayer stoppt Cyberattacke, die mutmaßlich chinesische Merkmale getragen haben soll), Reuters, 4. April 2019 (https://www.reuters.com/article/us-bayer-cyber/bayer-contains-cyber-attack-it-says-bore-chinese-hallmarks-idUSKCN1RG0NN).

[11] Die Zusammenarbeit zwischen I&O- und S&R-Teams wird nur in wenigen Unternehmen gefördert. Lesen Sie den Forrester-Bericht „Ransomware Is A Business Continuity Issue“ (Ransomware ist ein Problem der Geschäftskontinuität).

[12] Lesen Sie den Forrester-Bericht „Forrester's Guide To Paying Ransomware“ (Leitfaden zur Zahlung von Lösegeld).

[13] Beispiele sind NotPetya und andere Angriffe, die herkömmliche Sicherheitstools nicht stoppen konnten.

[14] Quelle: FINRA (https://www.finra.org/sites/default/files/SEA.Rule_.17a-4.Interpretations_0_0.pdf).

[15] Lesen Sie den Forrester-Bericht „The Forrester Wave™: Data Resiliency Solutions, Q3 2019“ (The Forrester Wave™: Lösungen für die Datenausfallsicherheit, 3. Quartal 2019).

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

Wir arbeiten mit Unternehmen und Technologieführern zusammen, um kundenorientierte Strategien zu entwickeln, die das Wachstum fördern.

PRODUKTE UND LEISTUNGEN

- Zentrale Forschung und Tools
- Daten und Analysen
- Zusammenarbeit mit Kollegen
- Einbeziehung von Analysten
- Beratung
- Ereignisse

Die Forschungsergebnisse und Erkenntnisse von Forrester sind auf Ihre Rolle und wichtige Geschäftsinitiativen zugeschnitten.

RELEVANTE ROLLEN

Marketing- und Strategieexperten

CMO
B2B-Marketing
B2C-Marketing
Kundenerfahrung
Kundeneinblicke
eBusiness und Channel-Strategie

Experten im Bereich Technologiemanagement

CIO
Anwendungsentwicklung und Anwendungsbereitstellung
Unternehmensarchitektur
- Infrastruktur und Betrieb

Sicherheit und Risiken
Beschaffung und Anbietermanagement

Experten der Technologiebranche

Analystenbeziehungen

KUNDENSERVICE

Informationen zu gedruckten Exemplaren oder elektronischen Nachdrucken erhalten Sie von der Kundenbetreuung unter +1 866-367-7378, +1 617-613-5730 oder unter clientsupport@forrester.com. Wir bieten Mengenrabatte und Sonderpreise für akademische und gemeinnützige Einrichtungen.