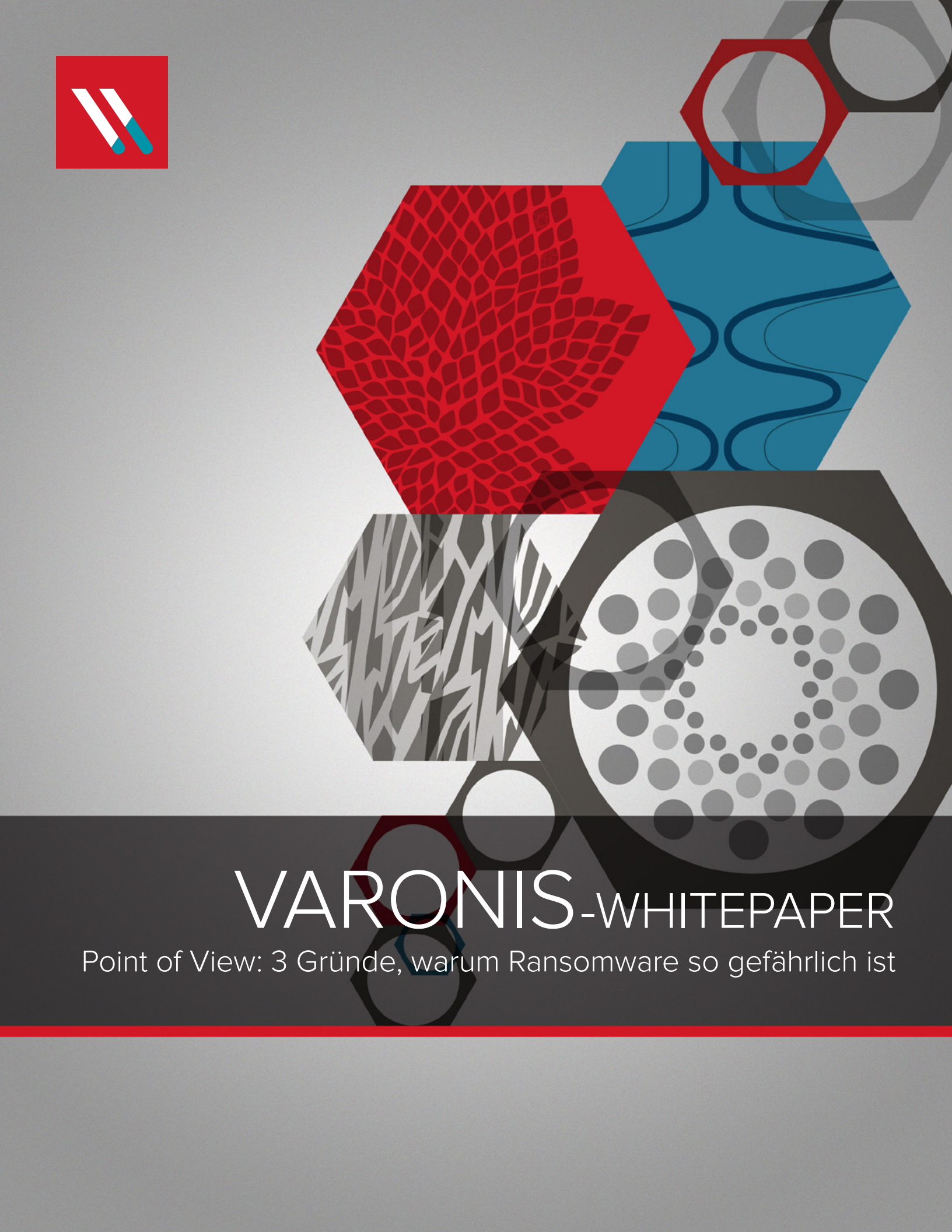

VARONIS-WHITEPAPER

Point of View: 3 Gründe, warum Ransomware so gefährlich ist

3 GRÜNDE, WARUM RANSOMWARE SO GEFÄHRLICH IST

GESCHICHTEN VON DER RANSOMWARE-FRONT

“WIR HABEN EINEN GANG HERUNTER GESCHALTET UND DEN STECKER DER MASCHINE GEZOGEN,”

erklärte der Leiter der Abteilung Informationssicherheit eines Holzproduktionsunternehmens im pazifischen Nordwesten der USA. Das war zwar mit Sicherheit nicht die technisch anspruchsvollste Lösung, um die Ransomware-Infektion und ihre Ausbreitung aufzuhalten, aber es hat die Bedrohung zu einem frühen Zeitpunkt gestoppt.

> *„Die Ransomware hat es durch unsere Firewall [neu und eine Next-Generation-Firewall] und das IDS geschafft sowie vorbei an den Meldungen unseres SIEM. Wir hatten auch zwei separate Programme [zur Malware-Erkennung] auf unseren Arbeitsplätzen im Einsatz.“*

Die Signatur dieser speziellen Malware-Variante war jedoch noch nicht bekannt, sodass der Code unbemerkt die Netzwerkgrenzen passiert hat und die End-Point-Sicherheitsmaßnahmen überwinden konnte. Und anschließend damit begonnen hat, Dateien auf den Fileshares zu verschlüsseln.

> *„Eine Varonis-Benachrichtigung wurde innerhalb von drei Minuten nach dem Ausbruch ausgelöst. Wir hatten zwar die Benachrichtigung aktiviert, mussten aber noch die automatische Reaktion konfigurieren, sodass wir die Maschine vom Strom genommen haben.“*

In diesem Fall war der Benutzer, der auf viele extrem sensible Informationen zugreifen konnte, der Leiter der Rechtsabteilung. Glücklicherweise konnte der Angriff gestoppt werden, bevor die Malware den Command-and-Control-Server (C&C) erreicht und dort die erfolgreiche Infektion bestätigt hätte. Darüber hinaus konnte mithilfe des DatAdvantage-Zugriffsprotokolls eine Liste der Dateien erstellt werden, die wiederhergestellt werden mussten.

Das ist nur eines der vielen Beispiele von Ransomware-Erfolgsgeschichten, die Varonis von seinen bestehenden und zukünftigen Kunden überall auf der Welt zu hören bekommt. Unternehmen und Organisationen aus alle Bereichen, vom Gesundheitswesen über Regierungsinstitutionen bis hin zu Finanzdienstleistern und Unternehmen aus der Produktion werden tagtäglich von neuen und immer heimtückischeren Ransomware-Varianten, wie CryptoLocker, angegriffen. Varonis führt jeden Monat hunderte von Risikobewertungen durch und ist in tausenden von Umgebungen installiert. Für viele dieser Kunden ist Varonis mittlerweile essentiell um diese Art von Angriffen zu verhindern, zu erkennen, einzudämmen und zu beheben.

Was Ransomware so heimtückisch macht, ist die Tatsache, dass sie so einfach Schwachstellen im Inneren der Sicherheitsgrenzen ausnutzen kann – ein Angriffspunkt bei so vielen Unternehmen und Organisationen.

Das sind 3 der Gründe, warum Ransomware so gefährlich ist:

1. Viele Unternehmen überwachen überhaupt nicht, wie Mitarbeiter Laufwerke verwenden – das sind riesige Datenspeicher, die das Ziel neuer Ransomware-Varianten sind. Sie können aber nur aufhalten, was Sie auch sehen. Deshalb ist es extrem schwierig, Ransomware aufzuspüren, ohne die Nutzung der Fileshares zu überwachen.

2. Noch schwerer wiegt jedoch die Tatsache, dass Benutzer in der Regel Zugriff auf deutlich mehr Dateien haben, als sie benötigen und viele der Dateien sogar sämtlichen Mitarbeitern zur Verfügung stehen. Das bedeutet, dass Ransomware nach dem Eindringen in ein System verheerenden Schaden anrichten kann. Selbst ein einzelner kompromittierter Benutzer kann so bereits große Datenmengen sperren.

3. Dazu kommt, dass die meisten Unternehmen keine Berichte darüber haben, wer wann welche Dateien verändert (oder verschlüsselt) hat. Es ist sehr aufwendig sicherzustellen, dass nichts verloren geht. Um sich von einem Angriff zu erholen, müssen meistens ganze Fileshares abgeschaltet werden, um dann die Dateien über Backups wiederherstellen zu können.

Im Januar 2016 war der County Council in Lincolnshire, Großbritannien, von einer Ransomware-Variante betroffen, die das gesamte Netzwerk für mehr als 24 Stunden lahm legte und im ganzen Land ein viel diskutiertes Thema war. Ein benachbarter Ort wurde sofort alarmiert, und dort warf man einen genaueren Blick auf die eigenen Systeme, um Schwachstellen zu identifizieren.

> *„Nach den Vorfällen in Lincolnshire sind wir jetzt sogar noch mehr auf der Hut.“*

Die Behörden im benachbarten Ort installierten Varonis und konnten so eine frische Infektionen umgehend melden und blockieren, weitere Schäden verhindern, und vermeiden, ebenfalls in den Nachrichten zu bekämpfen.

Die beste Art Ransonmware zu stoppen besteht darin, dass Benutzer nur Zugriff auf die Daten haben, die diese wirklich benötigen, und dass sämtliche Zugriffe überwacht und anaylsiert werden. Der Grund, dass Varonis so häufig als Reaktion auf Ransomware installiert wird, ist, dass die Varonis-Software beides kann: Varonis überwacht und analysiert alle Aktivitäten, sodass Sie Ransomware und andere Insider-Bedrohungen erkennen. Darüber hinaus können Sie aber auch Zugriffe sperren, wie beispielsweise globale Zugriffe, und übermäßige individuelle Berechtigungen intelligent reduzieren.

Kunden waren von der Effizienz der Varonis-Lösung überrascht, besonders im Vergleich zu anderen Lösungen, in die sie investiert hatten. Eine große westkanadische Bank kann über die letzten sechs Monate als Musterbeispiel dienen: Das Unternehmen investierte mehr als 500.000 USD für neue Sicherheitstools von verschiedenen Anbietern und musste dennoch feststellen, dass es der Erkennung oder Verhinderung von Angriffen kein Stück näher gekommen war.

> *„Unter all den anderen teuren Sicherheitsprodukten, die wir gekauft haben, ist DatAlert die Lösung, die alle Meldungen und Benachrichtigungen bei ungewöhnlichem Verhalten, insbesondere bei Ransomware, ausgibt und ausgegeben hat“, so Vertreter der Bank.*

ÜBER VARONIS

Varonis ist der führende Anbieter von Softwarelösungen zum Schutz von Daten vor Insiderbedrohungen und Cyberangriffen. Über eine neuartige Softwareplattform erlaubt Varonis es Unternehmen ihr umfangreiches Volumen an unstrukturierten Daten zu analysieren, abzusichern, zu verwalten und zu migrieren. Dabei ist Varonis spezialisiert auf die in Datei- und E-Mail-Systemen gespeicherten Daten, die wertvolle Informationen in Tabellen, Word-Dokumenten, Präsentationen, Audio- und Video-Dateien sowie E-Mails und Textdateien enthalten. Diese rasch wachsenden Daten enthalten in aller Regel finanzielle Informationen, Produktpläne, strategische Inhalte, geistiges Eigentum sowie hoch vertrauliche Inhalte wie beispielsweise Mitarbeiter- und Kundendaten oder sensible Patientendaten. IT-Abteilungen und kaufmännisches Personal setzen die Varonis-Software für eine Vielzahl unterschiedlicher Anwendungsfälle ein. Dazu gehören die Bereiche Datenschutz und Datensichertheit, Governance und Compliance, die Analyse des Benutzerverhaltens (UBA – User Behavior Analytics), das Archivieren von Daten sowie die unternehmensweite Suche danach und nicht zuletzt die Bereiche Dateisynchronisation und das Teilen und gemeinsame Nutzen von Daten.

Sie können alle Varonis-Produkte 30 Tage lang kostenlos testen. Unsere Systemtechniker bringen sie im Handumdrehen zum Laufen.

SCHNELL UND PROBLEMLOS

Unser kompetenter Servicetechniker übernimmt dabei die schwierigen Aufgaben für Sie: Einrichtung, Konfiguration und Analyse – mit konkreten Schritten wie Sie Ihre Datensicherheit verbessern.

BEHEBT BESTEHENDE SICHERHEITSLÜCKEN

Wir helfen Ihnen dabei, Sicherheitslücken zu beheben und einen Risikobericht basierend auf Ihren Daten zu erstellen.

NICHT-INTRUSIV

Wir bremsen weder Sie, noch Ihr System aus. Wir überwachen jeden Tag Millionen von Ereignissen, ohne die Leistung des Systems zu beeinträchtigen.

KOSTENLOSEN TEST JETZT STARTEN