arcserve®

Protect what's priceless.

IHR LEITFADEN FÜR EINE RANSOMWAREFREIE ZUKUNFT

EIN PROAKTIVER ANSATZ ZUR BEKÄMPFUNG DER RANSOMEWARE BEDROHUNG.

WHITE PAPER

RANSOMWARE IST ZU EINEM DER GRÖSSTEN GESCHÄFTSRISIKEN GEWORDEN UND STELLT DIE GRÖSSTE BEDROHUNG FÜR IT-UNTERNEHMEN DAR.

Ransomware ist zu einem der größten Geschäftsrisiken geworden und stellt die grösste Bedrohung für IT-Unternehmen dar. Es hat weltweit epidemische Ausmaße angenommen, wobei die Kosten bis 2021 auf 20 Milliarden Dollar geschätzt werden.[1]

Dennoch müssen diese Nachrichten für IT-Profis und Entscheidungsträger im Unternehmen nicht gleich verheerend sein. Während die Cyberkriminellen keine Anzeichen einer Schwächung zeigen, lassen Fortschritte bei der Bekämpfung von Cyberkriminalität und Disaster-Recovery-Technologien in Verbindung mit soliden IT-Management-Praktiken Unternehmen zurückschlagen.

Dieser Bericht untersucht die sich entwickelnde Bedrohung durch Ransomware, die Technologien und IT-Management-Praktiken, die zur Verteidigung eingesetzt werden, sowie einen vorausschauenden Ansatz zur Realisierung einer ransomwarefreien Zukunft.

KENNE DEINEN FEIND

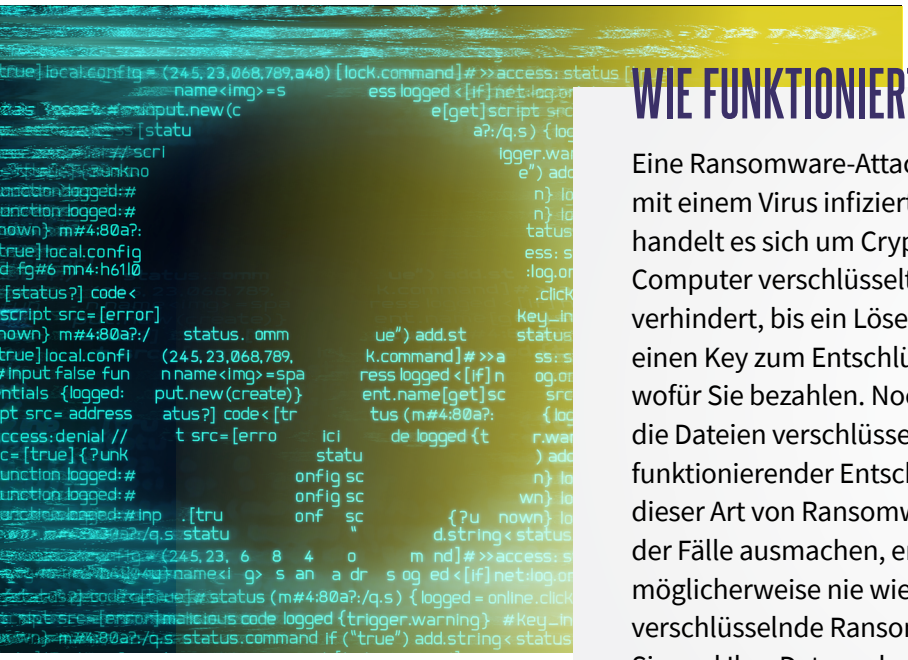
Der chinesische Militärstratege Sun Tzu empfahl klugerweise "Kenne deinen Feind". Um eine Strategie zur Sicherung von IT-Systemen vor Ransomware zu entwickeln, müssen Sie diese verstehen. Beginnen wir also damit, zu untersuchen, was Ransomware ist.

Daten sind das Herzblut Ihres Unternehmens. Sie repräsentieren Ihren betrieblichen Ablauf, wie er zwischen den Geschäftsbereichen stattfindet. Sie dokumentieren die Vergangenheit, kommunizieren den aktuellen Stand des Geschäfts und sind die Grundlage für Entscheidungen. Ohne sie ist es nicht übertrieben zu sagen, dass Sie keine Geschäfte machen können. Und das ist die Idee, aus der Ransomware Kapital schlägt.

Ransomware ist eine bösartige Software, die darauf ausgelegt ist, den Zugriff auf Ihre Computersysteme oder Daten zu verweigern, bis das Lösegeld bezahlt wurde. Sie kann Ihr Unternehmen vollkommen lahmlegen, oder, falls es sich zudem um Leakware oder Extortionware handelt, kann sie noch einen Schritt weiter gehen und drohen Ihre Daten zu exportieren und offenzulegen.

Jede Organisation mit wichtigen Daten, die auf Computern oder Netzwerken gespeichert sind, ist gefährdet - was heutzutage für fast jede Organisation gilt. Staats- und Kommunalverwaltungen, Strafverfolgungsbehörden, Gesundheitsorganisationen, Banken und Kreditkartenunternehmen sind allesamt große Ziele, mit denen die Identitätsdiebstahlindustrie den Markt anheizt, indem sie im Jahr 2018 den Verbrauchern belegte 14,7 Milliarden Dollar gestohlen hat.[2]

Es sind nicht nur große Organisationen betroffen, sondern Ransomware-Angriffe wiederfahren auch Verbrauchern und Körperschaften, kleinen und großen Unternehmen gleichermaßen.



WIE FUNKTIONIERT RANSOMWARE?

Eine Ransomware-Attacke findet statt, wenn ein Computer mit einem Virus infiziert wurde. Bei der meisten Ransomware handelt es sich um Cryptoware, die Dateien auf dem betroffenen Computer verschlüsselt und den Zugriff auf die Dateien so lange verhindert, bis ein Lösegeld gezahlt wird, im Austausch gegen einen Key zum Entschlüsseln der Dateien. Aber seien Sie vorsichtig, wofür Sie bezahlen. Noch gefährlicher ist gefälschte Crypto, die Dateien verschlüsselt und Lösegeld verlangt, ohne dass ein funktionierender Entschlüsselungskey ausgetauscht wird. Opfer dieser Art von Ransomware, die Schätzungen zufolge etwa 50 % der Fälle ausmachen, erhalten selbst nach Zahlung des Lösegeldes möglicherweise nie wieder Zugang zu ihren Dateien. Nicht verschlüsselnde Ransomware platziert einen Lock-Screen zwischen Sie und Ihre Daten, ohne diese direkt zu verschlüsseln.

Ransomware kann bestimmte Dateien oder das gesamte System über den Master Boot Record (MBR) eines Laufwerks oder Microsofts NTFS angreifen und dadurch das Betriebssystem am Hochfahren hindern. Ransomware vermeidet oft die Erkennung, indem sie ein Netzwerk wie z.B. HTTPS verschlüsselten Datenverkehr oder Tor nutzt. Im Gegensatz zu anderen Arten von Malware, die im Hintergrund agieren können, macht Ransomware, sobald sie in den betroffenen Host eingedrungen ist, ihre Anwesenheit bekannt, während sie nicht zurückverfolgbare Krypto-Währungen für die Lösegeldzahlung verlangt.

Es kann nur eine kleine, unbeabsichtigte Aktion erforderlich sein, die ein unschuldiger Benutzer ausführt, z. B. das Klicken auf einen infizierten Link, um den Computer zu befallen. Ransomware verbreitet sich in der Regel über Phishing-E-Mails, aber Cyberkriminelle verwenden zahlreiche Techniken, um ihre Opfer mit Ransomware zu befallen. Die Infizierung erfolgt in der Regel nach dem Öffnen eines E-Mail-Anhangs oder dem Klicken auf einen betrügerischen Link. Häufige Übertragungswege für die Verbreitung von Malware sind:

E -Mails und Textnachrichten mit Links welche Malware herunterladen oder einen Anhang mit Malware

Websites deren einziger Zweck darin besteht, Benutzer anzuziehen und sie dazu zu bringen, auf einen bösartigen Link oder einen Download zu klicken.

Malvertising oder böswillige Werbung, die im Wesentlichen Klick-Tricks sind, die zu unbeabsichtigten Downloads führen

Social Media die zwar mit vertrauenswürdigen Quellen verbunden scheint, aber schnell zu einem heimtückischen Cyberkriminellen führt. Ahnungslose Opfer nehmen die Infizierung direkt mit einer Social Media-Anwendung auf oder werden möglicherweise auf einen bösartigen Link oder Werbung gelenkt.

Mobile Apps die Nutzer freiwillig auf ihr Gerät herunterladen, ohne zu merken, dass es sich um eine Fälschung handelt und dass ein Virus übertragen wird, wenn das mobile Gerät das nächste Mal mit einem Computer verbunden wird.

Hacker werden immer raffinierter und zielen auf die Benutzer ab, indem sie infizierte Anhänge in einer E-Mail versenden, die scheinbar von jemandem aus ihrer Kontaktliste stammen. Und obwohl Nutzungsrichtlinien und Schulungen hilfreich sind, um das risikoreiche Verhalten von Endnutzern zu reduzieren, ist es unmöglich, diese Schwachstelle vollständig zu beseitigen, da die Einstiegspunkte nicht immer so offensichtlich sind. Bösartige Inhalte können Schwachstellen im Browser oder in den Plugins ausnutzen und ohne Wissen des Benutzers bösartigen Code ausführen. Einmal auf einem Host eingerichtet, kann sich eine Infektion leicht auf andere Computer im selben Netzwerk ausbreiten.

Cyberkriminelle ködern die Benutzer nicht nur um unwissentlich Ransomware herunterzuladen, sondern erhalten auch Zugang zu Systemen über das Internet, während niemand in der Nähe ist. Sie verwenden sowohl gewaltsame Methoden als auch im Dark Web gekaufte Zugangsdaten, um auf Ressourcen und Daten zuzugreifen und nutzen dabei Schwachstellen im Remote Desktop Protocol und in der Software aus.

Ein Bericht aus dem Jahr 2019 ergab, dass unter Unternehmen und Regierungsorganisationen die häufigsten Ziele für Ransomware hochwertige Vermögenswerte wie Server, Anwendungsinfrastruktur und Kollaborationstools sind. Während IT-Organisationen zu Recht den Trends und den kritischsten Schwachstellen die höchste Priorität einräumen, können ältere oder weniger kritische Schwachstellen nicht ignoriert werden. In dem Bericht machen ältere Schwachstellen (die drei Jahre oder älter sind) mehr als ein Drittel der Angriffe aus, wobei mehr als die Hälfte davon auf die weniger kritischen Schwachstellen entfallen.[3]

RANSOMWARE-ANGRIFFE VERURSACHEN IM DURCHSCHNITT FAST 10 TAGE AUSFALLZEIT[4]

Was sind die Auswirkungen einer Ransomware-Infektion?

Kontinuierliche Nachrichten über Ransomware-Angriffe und ein Ansturm von erschreckenden Statistiken haben Unternehmen bereits dazu veranlasst, aufmerksam zu werden und nach funktionierenden Datensicherheits- oder Datenschutzlösungen zu suchen. Die unmittelbare Folge eines Lösegeldangriffs ist eine erhebliche Unterbrechung des Geschäftsbetriebs, während Geräte und Systeme offline genommen werden, zur Desinfizierung und hoffentlich nahtlosen Wiederherstellung von sauberen Daten, was durch eine gut geplante Backup- und Disaster Recovery-Strategie ermöglicht wird. Ransomware-Angriffe verursachen im Durchschnitt fast 10 Tage Ausfallzeit.[4]

Obwohl das FBI von Lösegeldzahlungen abrät, berichtet es, dass 2018 mehr als 2,57 Millionen Dollar Lösegeld gezahlt wurden.[5] Im Durchschnitt kann ein Unternehmen mit durchschnittlichen Kosten von $133.000 pro Angriff rechnen - alles, um wieder Zugriff auf die eigenen Daten zu erhalten.[6] Und leider zahlen manche Opfer ohne Garantie dass sie ihre Dateien und Daten wiederherstellen können. Studien zeigen, dass Ransomware-Autoren in der Regel mehr als das Doppelte des Durchschnittsgehalts von Entwicklern verdienen die an legitimen Projekten arbeiten.[7] Es liegt auf der Hand, dass das was für Angreifer funktioniert, schlecht für Unternehmen und ihre professionellen IT-Mitarbeiter ist.

$2.57 MILLIONEN LÖSEGELD-ZAHLUNGEN[5]

$133,000 DURCHSCHNITTLICHE KOSTEN PRO ANGRIFF[6]

Unternehmen hoffen inständig, dass ihre Anti-Ransomware-Abwehr funktioniert. Aber selbst wenn sie das Schlimmste verhindern - oder zumindest teilweise verhindern - müssen sie möglicherweise immer noch mit Datenverlusten rechnen, die durch den Angriff entstanden sind. Die durchschnittlichen Verluste durch einen Angriff betragen etwa 8 Prozent der Daten.[8] Zusätzlich zu dem Versuch Lösegeld zu erhalten, können Angreifer Daten von einem kompromittierten Computer oder Server extrahieren und dabei sensible Daten, einschließlich Benutzernamen und Kennwörter, Zahlungsinformationen und E-Mail-Adressen von Kontakten, offenlegen. Moderne Ransomware greift Backup-Dateien auf Netzwerkfreigaben an und kann sogar Schatten-Kopien auf der Workstation löschen, um eine Wiederherstellung zu verhindern. Der Angriff und der daraus resultierende Datenverlust sind ein wirkungsvoller Doppelschlag, und die Risiken für den Ruf einer Firma können langfristig verheerende Auswirkungen haben, die ihre Vertrauenswürdigkeit stark beeinträchtigen.

> *"Cyberkriminelle werden immer raffinierter in ihren Taktiken, und scheinbar ist keine Branche vor Ransomware-Angriffen gefeit. Indem sie auf Backup-Systeme zielen, erhöhen Hacker die Chancen, dass kompromittierte Unternehmen Lösegeldzahlungen leisten, angesichts der schwerwiegenden Folgen von Datenverlust und Ausfallzeiten - die oft weit über die finanziellen Auswirkungen hinaus-gehen. IT- und Unternehmensleiter müssen auch die negativen Auswirkungen auf die Produktivität der Mitarbeiter, das Kundenvertrauen, den Ruf der Firma und die Einhaltung gesetzlicher Vorschriften berücksichtigen, wenn Systeme und Daten kompromittiert werden"*
>
> *- Oussama El-Hilali, Arcserve Chief Technology Officer*

Wie schützen IT-Experten ihre Organisationen vor Lösegeldforderungen?

Eine Vielzahl von Methoden wird eingesetzt, um Ransomware zu erkennen und wertvolle Systeme und Daten zu schützen, einschließlich:

- **Ransomware Schutz Software** um potenzielle Angriffe zu identifizieren und Eingriffe zu erkennen und zu verhindern, sobald sie geschehen.
- **Firewalls** um den unbefugten Zugriff auf einen Computer oder ein Netzwerk zu blockieren.
- **File Filters** and **Spam Filter** die Webseiten blockieren, bei denen der Verdacht auf Malware besteht und unerwünschte Anhänge daran hindern, in die E-Mail-Postfächer der Benutzer einzudringens.
- **Group Policy Software** die die Ausführung von Dateien aus lokalen Ordnern blockiert, die dann das System infizieren können.
- **Security Information and Event Management (SIEM)** Pakete die Einblicke in den Netzwerkverkehr gewähren, um Anomalien zu erkennen, die auf einen Verstoß hinweisen.
- **Backup Software** zum Schutz von Geschäftsdaten durch Kopien der Daten von Servern, Datenbanken, Desktops, Laptops und anderen Geräten.
- **File Integrity Monitoring** zur Verifizierung der Übereinstimmung zwischen der aktuellen und einer validierten Datei.
- **Antivirus and Anti-Malware Software** zum Verhindern, Erkennen und Entfernen von Malware.
- **Unified Threat Management (UTM)** Lösungen zur Bekämpfung verschiedener Bedrohungen mit einem zentralen Abwehrmechanismus und einer einzigen Konsole

Obwohl die oben genannten Punkte individuell wichtig und nützlich für Unternehmen sind, sind Organisationen ohne einen einheitlichen End-to-End-Ansatz in Bezug auf Ransomware einem größeren Risiko ausgesetzt. Die Angreifer von heute werden immer raffinierter und einfallsreicher. Angriffsstrategien kombinieren oft mehrere Techniken gleichzeitig und zielen gleichzeitig auf verschiedene Teile des IT-Netzwerks ab. Ransomware-Angriffe nutzen neue Malware-Varianten, um Antiviren-Programme zu umgehen. Wo liegen also die Fallstricke traditioneller Ransomware-Schutzstrategien?

Vielen Systemen fehlen wichtige Funktionalitäten.

Es war einfacher, das Malware-Problem anzugehen, als Exploits mit signaturbasierter Antivirentechnologie abgeglichen werden konnten. Da sich die Bedrohungen weiterentwickeln und unterschiedliche Angriffe auf gängige Schwachstellen beinhalten, ist es schwieriger geworden, die Bedrohungen mit Hilfe signaturbasierter Technologie zu identifizieren.

Darüber hinaus sind viele Datenschutzanbieter auf den Ransomware-Zug aufgesprungen und betonen „Cybersicherheits-Features", die in Wirklichkeit nur Datenanomalien erkennen, die mit Ransomware in Zusammenhang stehen können oder auch nicht. Und nachdem sie die Anomalie entdeckt haben, geben sie oft nur eine Warnung aus, anstatt etwas zur Lösung des Problems beizutragen.

Unterschiedliche Anwendungen sind schwer zu handhaben, was die Anfälligkeit erhöht.

Viele Unternehmen verwenden mehrere Tools und Anbieter für verschiedene Sicherheitsfunktionen zur Bekämpfung von Ransomware - zum Beispiel können sie zwei Anbieter für Firewalls, einen dritten für DLP- oder Webfilter, einen vierten für Backup und Disaster Recovery, einen fünften für Cloud-Backup für Rechenzentren und noch einen weiteren für mobiles Backup verwenden.

Die Verwendung separater Appliances und verschiedener Anbieter für unterschiedliche Sicherheitsaufgaben erschwert die Verfolgung und Verhinderung von Angriffen. Tools und Software erfordern Verwaltung und Updates, was es schwieriger macht, mit den neuesten Formen von Malware auf dem Laufenden zu bleiben, wenn mehrere Lösungen zusammengeschustert werden. Die Verwaltung mehrerer Anbieter und Lösungen erhöht Risiken, Schwachstellen und Fehler. Die Produktivität leidet und die Kosten steigen.

Heutzutage können Sie komplexe und veraltete Ransomware-Tools von unterschiedlichen Anbietern in eine einzige Lösung umwandeln, die eine umfassende Datensicherung und -wiederherstellung sowie den Schutz von neuronalen Netzwerken und Endgeräten vor unbekannter Malware, Exploits und Ransomware bietet.

IT-Fachleute brauchen auch IT-Managementpraktiken

Technologielösungen sind für die Cybersicherheit und den Schutz vor Ransomware von entscheidender Bedeutung - einschließlich Firewalls, Einbruchserkennungs- und Präventionssysteme sowie E-Mail-Sicherheit. Fortschrittliche Lösungen für integrierte Datensicherheit und -schutz sind ein wichtiger Beitrag zum Schutz von Organisationen. Gleichzeitig sind solide IT-Managementpraktiken unerlässlich.

Es ist wichtig zu erkennen, dass das Verhalten der Endbenutzer die größte Bedrohung darstellt. Unternehmen müssen IT-Managementkontrollen implementieren, die erkennen, wenn Mitarbeiter eine Richtlinie oder ein Verfahren umgehen. Die Verwaltungspraktiken sollten eine aktive Beteiligung der Benutzer beinhalten - d.h. es sollte kommuniziert werden, wie das Verhalten für die Sicherheit angepasst werden kann.

IT-Fachleute müssen auch ihr gesamtes IT-Portfolio berücksichtigen, um Risiken zu bewerten. Während jedes System anfällig für Angriffe ist, sind Kriminelle vor allem an wertvollen Informationen interessiert, die nicht ausreichend geschützt sind. Unternehmen müssen dem Ressourcenschutz Vorrang einräumen und ein proaktives IT-Management einschließlich Recovery Point Objectives (RPOs) einsetzen, um zu überlegen wie viel Datenverlust im Falle eines Ausfalls akzeptabel ist, und um die Abwehr zu stärken. Sie müssen wissen, über welche Ressourcen sie verfügen und wie diese konfiguriert sind, und sie müssen alle Änderungen streng kontrollieren.

Ein Rahmenwerk wie die Information Technology Infrastructure Library (ITIL) kann Unternehmen bei der Umsetzung von Best Practices für das IT-Management unterstützen. ITIL bietet Praktiken für das Konfigurationsmanagement, das Änderungsmanagement und das Release-Management als Schlüsselprozesse welche die Unternehmen, zur Stärkung der Cybersicherheit und gegen Ransomware-Bedrohung, beherrschen können.

IST FREI SEIN VON RANSOMWARE EINE REALISTISCHE PERSPEKTIVE?

Die Abwehr eines vielschichtigen Ransomware-Angriffs erfordert eine koordinierte Verteidigung, die die richtige Technologie mit soliden IT-Management-Praktiken kombiniert. Die ideale Lösung ist eine mehrschichtige, durchgängige Sicherheits- und Schutzlösung. Wenn eine IT-Abteilung eine erste und letzte Verteidigungslinie gegen Ransomware einsetzen kann, könnte sie die Bedrohung durch Lösegeldforderungen praktisch eliminieren und die Art und Weise verändern, wie sie die Daten des Unternehmens vor Erpressern, Hackern und Dieben schützt und sichert.

Eine kürzlich durchgeführte weltweite Umfrage unter IT-Fachleuten ergab, dass zwei von drei Befragten es für äußerst wichtig halten, Lösungen zu finden, die Datensicherheit und Datenschutz kombinieren.[9] Die Befragten halten dies sogar für wichtiger als Lösungen die KI zur Vorhersage von Katastrophen, oder solche die die Einhaltung von Vorschriften automatisieren, beinhalten.[10]

RANSOMWARE SCHUTZSTRATEGIEN

Hier skizzieren wir fünf Strategien zum Schutz vor Ransomware, die Ihnen helfen können, Ihr Unternehmen über reaktive Sicherheitsansätze hinauszuführen und Anti-Ransomware und andere Technologien zur Bedrohungsabwehr mit Disaster Recovery und Hochverfügbarkeitsfunktionen zu integrieren, um Cyberattacken zu neutralisieren.

1 Zugang aktiv verwalten

Erstellen Sie die notwendigen Kontrollen und Verfahren, um Anwendungen und Systeme vor unbefugten Benutzern zu schützen.

- Schränken Sie den Zugriff auf gängige Ransomware-Einstiegspunkte wie persönliche E-Mail-Konten und Social-Networking-Websites ein und verwenden Sie Webfilter am Gateway und am Endpunkt, um Phishing-Versuche für Benutzer zu blockieren, die durch einen Trick dazu gebracht werden, auf einen Link zu klicken.
- Nutzen Sie die Multi-Faktor-Authentifizierung und erweiterte Kennwortstandards und schließen Sie Kennwortanforderungen ein, wenn Benutzer mit Websites kommunizieren, die vom Proxy oder der Firewall nicht kategorisiert sind.
- Verwenden Sie Proxyserver und Werbeblockiersoftware und schränken Sie die Berechtigungen zum Installieren und Ausführen von Softwareanwendungen ein.
- Überprüfen und überwachen Sie Andere, die Remote-Zugriff auf das Unternehmensnetzwerk und Ihre Verbindungen zu Dritten haben, um sicherzustellen, dass diese die Best Practices für Cybersicherheit anwenden.
- Verwenden Sie Anwendungs-Whitelisten, um nur genehmigte Programme in einem Netzwerk ausführen zu lassen.

2 Verwalten der Systemkonfiguration über Angriffsvektoren hinweg

Implementieren Sie zentralisierte Verwaltungssysteme und -verfahren, die das gesamte Spektrum der Ransomware-Bedrohungen abdecken.

- Bewerten und kategorisieren Sie geschäftskritische Daten und implementieren Sie die physische und logische Trennung von Servern, Netzwerken und Datenspeichern.
- Stellen Sie sicher, dass Antiviren- und Anti-Malware-Lösungen in der Lage sind, ein- und ausgehende E-Mails automatisch zu aktualisieren und zu scannen, um Phishing zu erkennen, E-Mail-Spoofing zu verhindern und ausführbare Dateien zu filtern.
- Verwenden Sie ein zentralisiertes Patch-Management-System, um alle Endpunkte zu reparieren, sobald Schwachstellen entdeckt werden - auch auf mobilen Geräten, Betriebssystemen, Software und Anwendungen, in der Cloud und bei IoT.
- Setzen Sie signaturlose, Deep-Learning-, Anti-Exploit- und Anti-Ransomware-Technologien ein, die sowohl bekannte als auch unbekannte Malware erkennen.
- Implementieren Sie integrierte Endpoint Protection- und Business Continuity-Technologien, um die Abwehr von Bedrohungen zu beschleunigen und die sofortige Datenwiederherstellung zu ermöglichen.

- Sichern Sie Web-Applikationen und Web-Server mit Web-Application-Firewalls.
- Sperren Sie Skripte von per E-Mail versandten Microsoft Office-Dateien und ziehen Sie die Verwendung der Office Viewer-Software zum Öffnen von Office-Dateien in Betracht.
- Überprüfen Sie Ihr Netzwerk auf Systeme, die das Remote Desktop Protocol (RDP) verwenden, schließen Sie nicht verwendete Ports und nutzen sie die Zwei-Faktor-Authentifizierung.
- Erkennen und diagnostizieren Sie Verhaltensweisen, wie z. B. die Verschlüsselung von Massendateien, als bösartiges und blockierendes Verhalten.
- Fügen Sie in E-Mails von externen Quellen ein Warnbanner ein, das die Benutzer an die Gefahren beim Anklicken von Links und Öffnen von Anhängen erinnert.
- Verwenden Sie Unified Threat Management (UTM)-Appliances, die Firewall-, Gateway-Antivirus- und Intrusion-Detection- und Prevention-Funktionen kombinieren, um den Zugriff auf bekannte bösartige IP-Adressen zu blockieren.

3 Kombinieren von Lösungen für Datensicherheit und Datenschutz

Integrieren, testen und gewährleisten Sie umfassende Cybersicherheit und Datensicherung für einen End-to-End Schutz.

- Schützen Sie die Backup-Depots vor Malware, Ransomware und Zero-Day-Attacken.
- Stoppen und entfernen Sie Bedrohungen wie Malware und Ransomware aus den Backups.
- Bewahren Sie Datensicherungen auf separaten Geräten auf und verwenden Sie Offline-Speicher, wo sie von infizierten Geräten nicht direkt erreicht werden können.
- Sichern Sie virtuelle Maschinen, Cloud-Storage und Betriebssysteme auf der Basis Ihres Recovery Point Objectives (RPO) - unter Berücksichtigung des vertretbaren Datenverlusts im Falle eines Ausfalls.
- Verwenden Sie ein System, das es ermöglicht, mehrere Versionen von Backups zu speichern, falls eine Kopie der Backups verschlüsselte oder infizierte Dateien enthält.
- Integrieren Sie Appliances für Disaster Recovery und Anwendungsverfügbarkeit und nutzen Sie die Vorteile künstlicher Intelligenz für den Endpoint Schutz.
- Verwenden Sie Schwachstellen-Scans, SSL-Verschlüsselung und andere technische Kontrollen, um zu bestätigen, dass Backups durchgeführt werden.
- Wenden Sie die 3-2-1-Regel an, indem Sie drei Kopien Ihrer Daten erstellen, die auf zwei verschiedenen Medien gespeichert werden, wobei eine davon extern gespeichert wird.
- Testen Sie Backups routinemäßig auf Datenintegrität und um sicherzustellen, dass sie funktionsfähig sind.
- Testen Sie routinemäßig Daten und Disaster-Recovery-Prozesse, um die Verfügbarkeit sicherzustellen.

4 Einbindung der Benutzer durch Schulung und Kommunikation

Befähigen Sie die Anwender mit der nötigen Ausbildung und den erforderlichen Praktiken, um sich vor Ransomware-Bedrohungen zu schützen.

- Bieten Sie regelmäßige Sensibilisierungsschulungen und Informationen an, damit jeder in Ihrem Unternehmen die Bedrohung durch Ransomware versteht und mit den Sicherheitstechniken vertraut ist.
- Etablieren Sie Richtlinien zur Sicherheit und Ransonware-Prävention für Endnutzer.

- Weisen Sie die Benutzer darauf hin, keine verdächtigen E-Mails zu öffnen, nicht auf Links zu klicken oder Anhänge zu öffnen sowie vorsichtig zu sein, bevor sie unbekannte Websites besuchen, und auch ihren Browser zu schließen, wenn er nicht benutzt wird.
- Stellen Sie sicher, dass die Mitarbeiter wissen, wo und wie sie verdächtige Aktivitäten melden können.

5 Aufrechterhaltung und Test eines Business Continuity und Disaster Recovery Plans

Erstellen, testen und pflegen Sie die Praktiken, Verfahren und Technologie-Tools, um sicherzustellen, dass Anwendungen und Daten im Falle einer Katastrophe vollständig wiederhergestellt werden können.

- Erstellen Sie Notfall- und Sanierungspläne, die für die Wiederherstellung und Kontinuität des Geschäftsbetriebs entscheidend sind - unabhängig von der Ursache des Ausfalls.
- Führen Sie Risikoanalysen durch, die die Arten von möglichen Katastrophen klassifizieren und Prioritäten für die Wiederherstellung und die Geschäftskontinuität festlegen.
- Nutzen Sie sowohl Onsite- als auch Offsite-Lösungen für Disaster Recovery, Backup und Hochverfügbarkeit.
- Haben Sie einen Reaktionsplan für Vorfälle, der beinhaltet, was während eines Ransomware-Ereignisses zu tun ist, einschließlich des Trennens des infizierten Systems vom Netzwerk, um die Ausbreitung der Infektion zu verhindern und die Sensibilität der Daten zu bestimmen.
- Testen Sie den Plan - einschließlich der technologischen Systeme und Geräte - um sicherzustellen, dass der komplette Schutz gewährleistet ist.
- Melden Sie alle Infizierungen den zuständigen Autoritäten.

SIND SIE VORBEREITET AUF RANSOMWARE?

Laden Sie die **Selbstanalyse der Einsatzfähigkeit gegenüber Ransomware** herunter, um Ihre Fähigkeiten zu bewerten und einen Weg in eine ransomwarefreie Zukunft aufzuzeigen.

NEUE TECHNOLOGIEN VERSPRECHEN EINE RANSOMEWARE-FREIE ZUKUNFT

Seit Jahren suchen IT-Profis nach einer mehrschichtigen, durchgängigen Lösung für Datensicherheit und Datenschutz, um IT-Flexibilität und Ransomware-Prävention zu gewährleisten. Die gute Nachricht ist, dass es jetzt eine Lösung gibt, die genau das bietet - eine erste und letzte Verteidigungslinie gegen die Ransomware-Bedrohung.

Diese Lösung kombiniert die Arcserve Appliance Serie mit Sophos Intercept X Advanced für Server um einen mehrschichtigen Ansatz zu bieten, der vollständigen Datenschutz und Sicherheit bietet - alles auf einer einheitlichen Plattform.

Anwender profitieren von den umfassenden Funktionen eigenständiger Systeme, die die Beschaffung einzelner Komponenten einer Gesamtlösung überflüssig machen, indem sie eine zentrale Schnittstelle für Backup-Prozesse, Tools und Infrastruktur bereitstellen. Die Arcserve Appliances bieten auf einzigartige Weise flash-beschleunigten, deduplizierten Speicher, solide Serververarbeitung und Hochgeschwindigkeitsnetzwerke mit hoch redundanter Hardware und Cloud Services.

Fügen Sie den Endpoint-Schutz von Sophos Intercept X Advanced für Server hinzu und Sie erhalten eine End-to-End-Lösung, die signaturbasierte und signaturlose Malware-Erkennung, fortschrittliche künstliche Intelligenz/neuronales Netzwerk (deep learning), Anti-Exploit-Technologie und Anti-Ransomware-Technologien umfasst, um Schutz vor den verschiedensten Endpoint-Bedrohungen zu bieten.

Das Ergebnis: Eine unübertroffene Kombination aus "Alles in einem" - von der ersten bis zur letzten Stufe der Cybersicherheit, Datensicherung, Disaster Recovery und Hochverfügbarkeit, die alle in einer einzigen Lösung vereint sind, um jeden Infrastrukturbedarf vollständig abzudecken.

ZUSAMMENFASSUNG

Obwohl Ransomware ein erhebliches Geschäftsrisiko und eine bedrohliche Gefahr darstellt, ist die Zukunft vielversprechend. Denn heute können Unternehmen:

- **Integrierte Lösungen mit tiefgreifenden Schutzmaßnahmen** für fortschrittliches Backup, Disaster Recovery, Hochverfügbarkeit und Cybersicherheit bereitstellen;
- **IT-Praktiken** ermöglichen, die eine effektive Einbindung der Benutzer, Datenverwaltung und Disaster-Recovery-Praktiken ermöglichen, die einen Return on Investment (ROI) erzielen; und,
- **Eine Erste und Letzte Verteidigungslinie bereitstellen,** die das Erkennen von Bedrohungen beschleunigt und eine sofortige Wiederherstellung der gesicherten Daten ermöglicht.

Warum also den Status quo tolerieren? Warum eine Welt hinnehmen, in der Cyber-Erpresser, Hacker und Diebe Ransomware einsetzen, um unrechtmäßige Profite aus Unternehmen herauszuholen, die nur versuchen, ihre Geschäfte zu führen? Wehren Sie sich. Bewahren Sie Ihre Daten sicher auf. Nutzen Sie die heutige End-to-End-Schutztechnologie und solide IT-Management-Praktiken, um sicherzustellen, dass Sie und Ihr Unternehmen endlich eine ransomwarefreie Zukunft genießen können.

ÜBER ARCSERVE

Arcserve bietet außergewöhnliche Lösungen zum Schutz der wertvollen digitalen Bestände von Unternehmen, die einen vollständigen und umfassenden Datenschutz benötigen. Arcserve wurde 1983 gegründet und ist der weltweit erfahrenste Anbieter von Business Continuity-Lösungen, die Generationenübergreifende-IT-Infrastrukturen mit ihren Anwendungen und Systemen überall schützen, lokal und in der Cloud. Unternehmen in über 150 Ländern auf der ganzen Welt vertrauen auf die hocheffizienten, integrierten Technologien und das Know-how von Arcserve, um das Risiko von Datenverlusten und längeren Ausfallzeiten zu vermeiden und gleichzeitig die Kosten und die Komplexität der Datensicherung und -wiederherstellung um bis zu 50 Prozent zu reduzieren.

ÜBER SOPHOS

Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos als besten Schutz vor komplexen Bedrohungen und Datenverlusten. Sophos hat sich verpflichtet, komplette Sicherheitslösungen anzubieten, die einfach zu installieren, zu verwalten und zu handhaben sind und die niedrigsten Gesamtbetriebskosten der Branche bieten. Sophos bietet preisgekrönte Verschlüsselung, Endpoint Security, Web-, E-Mail-, Mobile-, Server- und Netzwerksicherheit, die von den SophosLabs - einem globalen Netzwerk von Threat Intelligence Centern - unterstützt wird.

QUELLENNACHWEIS:

1 https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

2 https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-report-fraudsters-seek-new-targets-and-victims-bear-brunt
https://www.aarp.org/money/scams-fraud/info-2019/survey-identity-fraud-decline.html

3 https://risksense.com/press_release/risksense-spotlight-report-exposes-top-vulnerabilities-used-in-enterprise-ransomware-attacks/

4 https://healthitsecurity.com/news/fbi-alerts-to-rise-in-ransomware-attacks-urges-victims-not-to-pay

5 https://pdf.ic3.gov/2018_IC3Report.pdf

6 https://www.sophos.com/en-us/press-office/press-releases/2018/01/businesses-impacted-by-repeated-ransomware-attacks-according-to-sophos-global-survey.aspx

7 https://twitter.com/CarbonBlack_Inc/status/925348051782373382

8 https://healthitsecurity.com/news/fbi-alerts-to-rise-in-ransomware-attacks-urges-victims-not-to-pay

9 Arcserve EMEA Survey, July 31, 2019

10 Arcserve EMEA Survey, July 31, 2019

Für mehr Informationen zu Arcserve, **besuchen Sie arcserve.com**