arcserve®

Protect what's priceless.

ANALYSE DER EINSATZFÄHIGKEIT GEGENÜBER RANSOMWARE

BEWERTEN SIE IHRE FÄHIGKEITEN UND WEISEN SIE DEN WEG IN EINE RANSOMWAREFREIE ZUKUNFT.

BEWERTUNG

BEWERTEN SIE IHRE FÄHIGKEITEN UND WEISEN SIE DEN WEG IN EINE RANSOMWAREFREIE ZUKUNFT.E

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]

Datensicherheitsmanagement ist ein wesentlicher Bestandteil einer guten IT-Verwaltung, insbesondere im Hinblick auf den Schutz kritischer Geschäfts- und Personendaten vor Ransomware.

Diese Bewertung kann Ihnen helfen, Lücken in Ihrer IT schnell zu erkennen und die Weichen für eine Ransomware freie Zukunft zu stellen.

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

RANSOMWARE-FREE EINE FÄHIGKEITS-REIFEGRAD BEWERTUNG

Anleitung

Führen Sie die Bewertung anhand der nachstehenden Punktekarte des **Capability Maturity Model**[2] (CMM) durch. Die Punktekarte beschreibt einen fünfstufigen Evolutionspfad zunehmend organisierter und systematisch reiferer Prozesse. Für jedes der Elemente des ransomwarefreien Konzepts können Sie den Reifegrad Ihrer Organisation bewerten und Ihre Prioritäten berücksichtigen.

Reifegrad	Reifegrad Level	Beschreibung
0	Kein Konzept	Kein Nachweis eines Konzeptes im Unternehmen vorhanden
1	Bewusstsein für das Konzept	Eingeschränktes Verständnis des Konzeptes, mit informellen Prozessen und Verfahren
2	Wiederholbares Verfahren	Ein Basisverfahren ist mit einigen unterstützenden Unterlagen vorhanden.
3	Standardisier-tes Verfahren	Das Verfahren wird im gesamten Unternehmen eingesetzt, wobei eine gemeinsame Sprache, Definitionen, Rollen und Verantwortlichkeiten vorhanden sind.
4	Verwaltetes Verfahren	Das Verfahren wird in der gesamten Organisation mit einer gemeinsamen Sprache, Definitionen, Rollen und Verantwortlichkeiten eingesetzt, und Abweichungen werden in der gesamten Organisation basierend auf der geschäftlichen Bedeutung verwaltet.
5	Operatives Verfahren	Das Verfahren wird in der gesamten Organisation mit einer gemeinsamen Sprache, Definitionen, Rollen und Verantwortlichkeiten eingesetzt und Abweichungen werden in der gesamten Organisation auf der Grundlage der geschäftlichen Bedeutung verwaltet. Regelmäßige Überprüfungen bestätigen, dass die Kriterien erreicht wurden.

[2] The Capability Maturity Model (CMM) was developed for the U.S. Department of Defense Software Engineering Institute (SEI) in 1986 located at Carnegie Mellon University in Pittsburgh, Pennsylvania.

Markieren Sie das Feld, das am besten zu Ihrem Firmenprofil passt.

1 Zugang aktiv verwalten

Verwalten wir effektiv den Zugang und die Kontrollen in unserem gesamten Systemportfolio?

AKTIONEN	KEIN KONZEPT	BEWUSSTSEIN	WIEDERHOLBAR	STANDARTISIERT	VERWALTET	OPERATIV
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 Endpoint, um Phishing-Versuche zu blockieren, bei denen Benutzer dazu verleitet werden, auf einen Link zu klicken.						
Verwenden Sie Multi-Faktor-Authentifizierung und erweiterte Kennwort Standards und schließen Sie Passwortanforderungen ein, wenn Benutzer mit Websites kommunizieren, die nicht durch den Proxy oder die Firewall kategorisiert sind.						
Nutzen Sie Proxyserver und Werbeblockade-Software und schränken Sie die Rechte zur Installation und Ausführung von Softwareanwendungen ein.						
Überprüfen und beobachten Sie Andere, die Fernzugriff auf das Netzwerk des Unternehmens und den Verbindungen zu Dritten haben, um sicherzustellen, dass diese die Best Practices für Cybersicherheit anwenden.						
Verwenden Sie eine Anwendungs-Whitelist, um nur genehmigte Programme in einem Netzwerk laufen zu lassen.						

2 Verwalten der Systemkonfiguration über Angriffsvektoren hinweg

Haben wir ein zentralisiertes Management und einen End-to-End-Ansatz entwickelt, welche das gesamte Spektrum möglicher Angriffe abdecken?

AKTIONEN	KEIN KONZEPT	BEWUSSTSEIN	WIEDERHOLBAR	STANDARTISIERT	VERWALTET	OPERATIV
Bewerten und kategorisieren Sie geschäftskritische Daten und implementieren Sie die physische und logische Trennung von Servern, Netzwerken und Datenspeichern.						

AKTIONEN	KEIN KONZEPT	BEWUSSTSEIN	WIEDERHOLBAR	STANDARTISIERT	VERWALTET	OPERATIV
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

Bietet unsere IT-Konfiguration umfassenden Endpoint-Schutz, Datenverfügbarkeit und Cybersicherheit?

AKTIONEN	KEIN KONZEPT	BEWUSSTSEIN	WIEDERHOLBAR	STANDARTISIERT	VERWALTET	OPERATIV
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

Binden wir unsere Nutzer vollständig in die Praktiken ein, die sie zum Schutz vor Ransomware-Bedrohungen benötigen?

AKTIONEN	KEIN KONZEPT	BEWUSSTSEIN	WIEDERHOLBAR	STANDARTISIERT	VERWALTET	OPERATIV
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

Sind wir in der Lage, unsere Anwendungen und Daten im Falle einer Katastrophe wiederherzustellen und betriebsbereit zu machen?

AKTIONEN	KEIN KONZEPT	BEWUSSTSEIN	WIEDERHOLBAR	STANDARTISIERT	VERWALTET	OPERATIV
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.						
Implementieren 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.						
Melden Sie alle Infizierungen den zuständigen Autoritäten.						

ZUSAMMENFASSUNG DER ANALYSE

Wie gut sind wir angesichts der fünf Ransomware-Verfahren auf eine lösegeldfreie Zukunft vorbereitet?

Reifegrad	Reifegrad Level	Beschreibung	Was ist unser Gesamtreifegrad?
0	Kein Konzept	Kein Nachweis eines Konzeptes im Unternehmen vorhanden	
1	Bewusstsein für das Konzept	Eingeschränktes Verständnis des Konzeptes, mit informellen Prozessen und Verfahren	
2	Wiederholbares Verfahren	Ein Basisverfahren ist mit einigen unterstützenden Unterlagen vorhanden.	
3	Standardisier-tes Verfahren	Das Verfahren wird im gesamten Unternehmen eingesetzt, wobei eine gemeinsame Sprache, Definitionen, Rollen und Verantwortlichkeiten vorhanden sind.	
4	Verwaltetes Verfahren	Das Verfahren wird in der gesamten Organisation mit einer gemeinsamen Sprache, Definitionen, Rollen und Verantwortlichkeiten eingesetzt, und Abweichungen werden in der gesamten Organisation basierend auf der geschäftlichen Bedeutung verwaltet.	
5	Operatives Verfahren	Das Verfahren wird in der gesamten Organisation mit einer gemeinsamen Sprache, Definitionen, Rollen und Verantwortlichkeiten eingesetzt und Abweichungen werden in der gesamten Organisation auf der Grundlage der geschäftlichen Bedeutung verwaltet. Regelmäßige Überprüfungen bestätigen, dass die Kriterien erreicht wurden.	

Was sind unsere nächsten Schritte?

SPRECHEN SIE MIT EINEM RANSOMWARE-EXPERTEN!

Erkunden Sie die Ransomware Best Practices und lassen Sie sich von unseren Experten dabei unterstützen alle Lücken zu identifizieren, die Sie für eine lösegeldfreie Zukunft schließen müssen. **Beratungstermin vereinbaren.**

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