5 Strategien gegen Ransomware

03.05.2022, 17:22 | IT, New Media & Software

Pressemitteilung von: *Attivo Networks*
Presseagentur: *Prolog Communications GmbH*

Manchmal bewahrt Ransomware Temposünder vor Bußgeldzahlungen, weil die zuständige Behörde nicht auf ihre Daten zugreifen kann wie jüngst im Landkreis Ludwigslust-Parchim.

Aber wenn wie 2021 im Landkreis Anhalt-Bitterfeld gar nichts mehr geht, hat niemand Grund zur Freude. Ransomware-Attacken werden nicht nur immer häufiger, sondern auch immer dreister und vor allem komplexer - und sie sind sehr häufig erfolgreich. Wie Behörden und Unternehmen sich am besten auf Ransomware-Angriffe vorbereiten und sich dagegen schützen können, ist eine schwer zu beantwortende Frage, da es keine einfachen Einheitslösungen für das Problem gibt. Attivo Networks erläutert 5 bewährte Strategien gegen Ransomware und ihre Folgen, die zwar auch keine hundertprozentige Sicherheit garantieren, aber die Wahrscheinlichkeit und die Auswirkungen solcher Angriffe erheblich

reduzieren können.

Multifaktor-Authentifizierung

Die Multifaktor-Authentifizierung (MFA) wird nicht alle Probleme eines Unternehmens lösen, aber sie ist eine relativ einfache Möglichkeit, eine zusätzliche Sicherheitsebene zu schaffen. MFA ist zwar nicht narrensicher, macht es einem Angreifer aber deutlich schwerer, gestohlene Zugriffsdaten zu verwenden, um einen Brückenkopf im Netzwerk des Opfers zu etablieren. Umso mehr, als viele Mitarbeiter dieselben Passwörter für mehrere Konten verwenden. Wenn MFA implementiert ist, sind selbst gültige Anmeldedaten für Angreifer nutzlos, wenn sie nicht auch die zweite Form der Authentifizierung kompromittieren können.

Identity Management

Die Multifaktor-Authentifizierung kann dazu beitragen, Benutzerkonten zu schützen, aber nicht helfen, wenn ein Mitarbeiter eine Phishing-E-Mail öffnet und auf einen verdächtigen Link klickt oder einen bösartigen Anhang herunterlädt, der auf ein ungesichertes System abzielt. Auch bei einem Zero-Day-Exploit ist MFA nutzlos, da der Angreifer die Notwendigkeit, ein Passwort zu knacken, umgangen hat und stattdessen direkt in das Netzwerk eingedrungen ist. Über das Active Directory können sie dann in der Regel ihre Privilegien erhöhen und neue, wertvolle Ziele identifizieren. Netzwerkbetreiber benötigen daher Tools, die frühzeitig Alarm schlagen, wenn ein Angreifer eine Anfrage stellt, und auch falsche Informationen zurückgeben, um zu verhindern, dass er den Endpunkt kompromittiert. Zudem sollten sie laut Attivo Werkzeuge benutzen, die Schwachstellen und Angriffspfade im Zusammenhang mit Anmeldedaten und privilegierten Konten aufzeigen.

Netzwerke segmentieren

Die Segmentierung von Netzwerken erleichtert es den Sicherheitsverantwortlichen, Angreifern Köder anzubieten, die sie in eine Falle locken, in der sie keine nützlichen Daten gewinnen können, aber ihre Vorgehensweise preisgeben.

Zero Trust - eher Reise als Ziel

"Zero Trust ist heute ein beliebtes Schlagwort, aber es ist wichtig zu verstehen, dass echtes Zero Trust eher eine Reise ist als ein Ziel.", so Jens Wollstädter, Regional Manager DACH von Attivo Networks. "Hier geht es weniger um Technik als um eine Reihe von Grundsätzen, die auf der Annahme fußen, dass das eigene Netzwerk bereits kompromittiert wurde." Aktivitäten innerhalb des Netzwerks sollten laut Attivo daher durch diese Brille betrachtet werden: Wenn eine Identität versucht, auf bestimmte Informationen oder Bereiche des Netzwerks zuzugreifen, sollte diese Anfrage validiert und authentifiziert werden, bevor sie gewährt wird. Die Annahme einer Sicherheitsverletzung bedeutet, dass Unternehmen immer nach Angreifern in ihrer Umgebung suchen sollten, in Benutzerkonten, Active Directory, Anwendungen, Netzwerkressourcen und an vielen anderen Stellen. Wenn Angreifer gezwungen sind, ihre Aktionen bei jedem Schritt zu rechtfertigen, wird es für die Netzwerkabwehr viel einfacher, verdächtige Aktivitäten zu erkennen.

Aktive Verteidigung implementieren

Aktive Verteidigungsstrategien können dazu beitragen, Verteidigern gegenüber Angreifern in eine bessere Position zu bringen. Sowohl MITRE als auch NIST (National Institute of Standards and Technology) haben erkannt, wie wichtig es ist, Angreifer in Fallen zu locken, anstatt einfach darauf zu warten, ihre Anwesenheit zu entdecken. Verteidiger können heute wichtige Daten, Konten und Netzwerkfreigaben verstecken und Angreifer mit Hilfe von Täuschungsmanövern in Umgebungen locken, wo sie sicher überwacht und untersucht werden können.

Verantwortlicher für diese Pressemitteilung:

Attivo Networks
Herr Jens Wollstädter
Fremont Boulevard 46601

94538 Fremont
USA

fon ..: +49 89 800 77-0
web ..: https://attivonetworks.com
email : attivo@prolog-pr.com

Pressekontakt:

Prolog Communications GmbH
Herr Achim Heinze
Sendlinger Str. 24
80331 München

fon ..: +49 89 800 77-0
web ..: http://www.prolog-pr.com
email : achim.heinze@prolog-pr.com

News-ID: 1228450 • Views: 506 (Stand: 01.05.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/1228450/5-Strategien-gegen-Ransomware.html