carmasec

security. done. right.

Whitepaper 09/2019

Risiko und Vertrauen: Mit dem CARTA-Ansatz die Herausforderungen digital-vernetzter Unternehmen bewältigen

Wenn Personen im Netzwerk unbemerkt Schaden verursachen

Klassische Sicherheitsarchitekturen sind regelmäßig nicht mehr wirkungsvoll genug für Unternehmen, die ihre Geschäfts- und IT-Prozesse zunehmend digitalisieren und vernetzen. Auch wenn es gängige Praxis war, reichte es in der Vergangenheit nicht aus, den Zugang zum Firmennetzwerk ausschließlich unternehmenseigenen Geräten zu erlauben, um sich vor Angriffen zu schützen.

Häufig wird darüber hinaus unterschätzt, dass Angriffe auf die IT-Sicherheit auch von Nutzern ausgehen können, die bereits Zugang zum internen Netzwerk des Unternehmers haben. Hierunter fallen sowohl Mitarbeiter, die dem Unternehmen vorsätzlich schaden wollen als auch externe Angreifer, die sich mittels zuvor ausgespähter Daten Zugang zum internen Netzwerk verschaffen.

In beiden Fällen können bestehende IT-Sicherheitssysteme das Risiko oftmals weder erkennen noch die damit verbundenen Bedrohungen unterbinden, da diese Nutzer bereits beim “Betreten” des Unternehmensnetzwerks als gefahrlos eingestuft werden. Sind diese Personen einmal im Netzwerk angemeldet, können sie über einen längeren Zeitraum unbemerkt Schäden verursachen.

Die Schwächen klassischer Sicherheitsarchitekturen

Konventionelle Sicherheitsansätze konzentrieren sich bislang auf die Vorhersage und Prävention von Bedrohungen, hauptsächlich mit Hilfe so genannter „Intrusion Detection- und Prevention-Systeme“ (IDS/IPS). Diese Systeme überwachen den Datenverkehr eines Netzwerks und gleichen ihn mit einer Liste bekannter bösartiger Muster ab. Sobald eine Übereinstimmung erkannt wird, lösen diese Systeme einen Alarm aus oder blockieren den Zugriff. Erkennungsmethoden dieserart werden auch als „Blacklisting“ bezeichnet. „Blacklists“ müssen kontinuierlich aktualisiert werden, sobald neue Bedrohungen auftreten.

Aufgrund der schnellen technologischen Entwicklung und dem damit einhergehenden Wachstum der Risiken der Digitalisierung ist dieser Ansatz stets reaktiv und bedingt einen enormen zeitlichen Verzug zur Erkennung von Angriffen und der Einleitung von entsprechenden Gegenmaßnahmen. Ein weiterer Nachteil der bisherigen Verteidigung gegen Cyber-Angriffe, die sich hauptsächlich auf ID-/IP-Systeme stützt, besteht darin, dass der Datenverkehr an Netzwerkübergabepunkten („Gateways“) im Fokus steht, anstatt sich auf systeminterne Aktivitäten zu konzentrieren. Somit können Angriffe erst erkannt werden, wenn diese bereits zu auffälligen Aktivitäten im Netzwerk führen. Angriffe genau dieser Art haben aber oft schwerwiegende Folgen für das attackierte Unternehmen und sollten im Idealfall zuvor verhindert werden.

AUF EINEN BLICK

- Konventionelle Sicherheitsansätze konzentrieren sich auf die Vorhersage und Prävention von Bedrohungen. In Anbetracht der wachsenden digitalen Risiken, können Unternehmen bei diesen Ansätzen oftmals nur reaktiv und mit enormer Verzögerung Angriffe erkennen und Maßnahmen gegen sie einleiten.
- CARTA stellt einen neuartigen Ansatz dar, in dem alle system- und prozessübergreifenden Transaktionen im Unternehmen automatisiert, dauerhaft kontrolliert und selbstlernend analysiert werden. Nicht einzelne Ereignisse sondern die Abfolge von Ereignissen werden bewertet, so dass Angriffe zuverlässig erkannt und vermieden werden.
- Die Etablierung von Vertrauenskultur und funktionierendes Risikomanagement im Unternehmen stellt eine zwingende Bedingung dar; Geschäftsmodelle in der Digitalisierung setzen den reibungslosen und dynamischen Transfer von Daten voraus, der nicht behindert werden darf, wie sie durch Kontrollinstanzen in konventionellen Sicherheitsansätzen verursacht werden.

Gartners CARTA als Antwort auf veränderte Gefahren

Das weltweit renommierte Marktforschungs- und Beratungshaus Gartner, das besonders für seine Bewertung von Technologie-Trends große Anerkennung genießt, hat 2017 einen Ansatz entwickelt, der die zuvor genannten Schwächen einer klassischen Sicherheitsarchitektur überbrücken will. Die Lösung der Trendforscher sieht eine automatische Analyse sämtlicher Vorgänge in einem Unternehmensnetzwerk und eine damit verbundene dynamische Regelung für den Zugang zu einzelnen Systemen oder Daten vor.

Dieser methodische Ansatz heißt CARTA und steht für „Continuous Adaptive Risk and Trust Assessment“, das ins Deutsche als “Kontinuierliche und adaptive Risiko- und Vertrauensbewertung” übersetzt werden kann. CARTAs zugrundeliegende Philosophie besagt, dass bestimmte Transaktionen in der digitalen Welt des modernen Geschäftsverkehres zulässig sein müssen, für die bisher keine vollständige Sicherheit gewährleistet werden konnte. Außerdem sollen zugrundeliegende Sicherheitsmechanismen dieser Transaktionen kontinuierlich weiterentwickelt und optimiert werden. Mit anderen Worten: Unternehmen, die in einem hochgradig dynamischen Daten- und Informationsumfeld sowie deren Beschäftigte in flexiblen, dezentralen und agilen Arbeitsumgebungen tätig sind, muss ein identifiziertes und kalkuliertes (Rest-)Risiko eingehen – und gleichzeitig Vertrauen aufbringen können.

„Whitelisting“ statt „Blacklisting“

Gartner empfiehlt den Aufbau und Betrieb einer automatisierten, dauerhaften, system- und prozessübergreifenden Analyse aller Transaktionen im Unternehmen. CARTA kombiniert dabei die Kontrolle von bereits als schädlich identifizierten Verhaltensweisen und Aktivitäten, die grundsätzliche Überwachung von Systemereignissen sowie die dauerhafte Überprüfung auf Abweichungen von einem vordefinierten „gutmütigen“ Verhalten („Whitelisting“). So wird sichergestellt, dass Anomalien erkannt und Angriffe abgewehrt werden können. In diesem Rahmen werden Entscheidungen auf Grundlage einer systematischen Bewertung von Risiko und Vertrauen getroffen und kontinuierlich an den Kontext und die Erkenntnisse angepasst, die aus jeder Interaktion gewonnen werden. Das Grundkonzept von CARTA baut auf einer “Adaptiven Sicherheitsarchitektur” (ASA) auf, die in vier Phasen gegliedert ist: Vorhersage, Prävention, Erkennung und Reaktion. Durch diesen gesamtheitlichen mehrstufigen Ansatz kann die Erkennungsrate von Anomalien und Angriffsmustern deutlich gesteigert werden.

GARTNER INC.

1979 gegründet ist Gartner ein weltweit führendes Forschungs- und Beratungsunternehmen, das Marktforschungsergebnisse und Analysen über Entwicklungen in der IT anbietet. Mittlerweile setzt das Unternehmen geschätzte 3,3 Milliarden US-Dollar um und gilt in der IT-Branche sowohl als führender Anbieter von Trendforschung als auch maßgebend für eigene Methoden und Modelle zu IT-Sicherheit.

Während ASA sich auf die Anpassungsfähigkeit der Architektur fokussiert, integriert CARTA auch den Entscheidungsprozess in das Konzept; so wird die Sicherheit des Systems permanent überwacht und an die sich ändernden Umstände angepasst. Risiken werden nicht mehr anhand eines Ereignisses, sondern anhand der Abfolge von Ereignissen konstant bewertet. Daraus ergeben sich im Wesentlichen drei Ziele von CARTA:

1. Die kontinuierliche und automatisierte Risikobewertung durch selbstlernende und anpassungsfähige Regelsätze
2. Eine zuverlässige Erkennung und Vermeidung von Angriffen, zudem eine behelfsweise Minderung der Auswirkungen von Angriffen
3. Die Einbeziehung externer Risikofaktoren, eine Unterstützung moderner IT-Praktiken wie Cloud und Container sowie adaptiver Richtlinien und diverser Erkennungsmethoden

So funktioniert CARTA

Intelligente Algorithmen sind hierbei so programmiert, dass permanent sämtliche Daten- und Nutzerbewegungen innerhalb eines Netzwerks in Echtzeit analysiert und somit alle zugreifenden Geräte nach ihrer Vertrauenswürdigkeit bewertet werden. In der Praxis könnte ein Angriffsschutz durch CARTA so aussehen, dass beim Download von Dateien aus dem internen Netzwerk geprüft wird, wie viele und welche Daten die Nutzer herunterladen und zu welchem Zeitpunkt. Sobald hierbei ein gewisser Wert überschritten wird

> „Zugleich ist CARTA ein substanzieller Denkanstoß für Entscheider in Unternehmen, ihre Kultur, Prozesse und Technologien zu hinterfragen und zu optimieren."
>
> *- Carsten Marmulla, Geschäftsführer*

oder eine Unstimmigkeit beim Download-Verhalten im Vergleich zu früheren Zugriffen eines Nutzers auffällt, unterbindet das System den Datentransfer und informiert sofort einen verantwortlichen Mitarbeiter. Der Schlüssel hinter dem CARTA-Ansatz ist Machine Learning, gemeinsam mit einer großen Datenbasis (Big Data), aus der die zugrundeliegenden Informationen geschöpft werden können. Die Daten werden also kontinuierlich nach Anomalien untersucht, die Auskunft über zweifelhafte Vorgänge im Unternehmensnetzwerk geben. Die Flexibilität einer adaptiven Sicherheitsarchitektur und im Besonderen CARTA können dazu beitragen, das Ziel eines sicheren Systems zu erreichen, das vor allem für langfristige und komplexe Projekte von großem Interesse ist.

Fazit & Ausblick

Laut Analysten sind CARTA-Ansätze langfristig betrachtet ressourcenschonend. Die Herausforderung des Konzepts besteht jedoch in der überzeugenden Praxistauglichkeit. Grundsätzlich aber dürfte eine permanente Big-Data-Analyse von Netzwerkvorgängen die Reaktionszeit nicht nur nach einem Sicherheitsangriff deutlich reduzieren. Eine solche kontinuierliche Analyse erlaubt ein automatisches Eingreifen durch die Sicherheitssysteme während eines aktiven Angriffs. In der eigenen Prognose gibt Gartner an, dass bis 2020 25 Prozent der neuen digitalen Geschäftsinitiativen einen CARTA-Strategie-Ansatz übernehmen werden.

Als Voraussetzung dafür gilt in erster Linie die Etablierung einer Vertrauenskultur im Unternehmen. Diese bildet das Gegenstück zur Kontrollkultur, die zahlreiche Jahre maßgeblich für die von Industrialisierung geprägten Betriebe war. Eine Stechuhr am Ein- und Ausgang einiger Arbeitsplätze funktioniert mitunter nicht mehr in Unternehmen, die ein modernes, digitales Geschäftsmodell präferieren.

Analog verhalten sich konventionelle Sicherheitsarchitekturen, in denen Personen sowohl beim Eintreten als auch Verlassen eines geschlossenen IT-Systems kontrolliert werden. Geschäftsmodelle im Zuge der Digitalisierung funktionieren derweilen dynamischer und verzweigter, denn Daten müssen schnell sowie reibungslos über Unternehmensgrenzen hinweg transferiert werden.

Der CARTA-Ansatz bietet vor diesem Hintergrund nicht nur ein technisches Konzept für eine innovative Sicherheitsarchitektur, die im Zeitalter der Digitalisierung in Betrieben konstant relevanter wird. Zugleich ist er ein substanzieller Denkanstoß für Unternehmen wie auch deren Entscheider, ihre Kultur, Prozesse und Technologien zu hinterfragen und zu optimieren. Diese drei Aspekte sind es, die hauptsächlich dazu beitragen, das Fundament für ein digitales Geschäftsmodell zu legen.

carmasec
security. done. right.

IHRE ANSPRECHPARTNER

Carsten Marmulla
Geschäftsführer

Jan Sudmeyer
Geschäftsführer

www.carmasec.com
xing.carmasec.com
contact@carmasec.com
twitter.carmasec.com
+49 (0) 201 426 385 900
linkedin.carmasec.com

Behalten Sie Ihre Cybersicherheit im Blick

Melden Sie sich für unseren Newsletter an:
www.carmasec.com/newsletter