NEVIS zeigt Anomalie-Erkennung und „Mobile Authentication“

Die NEVIS Security Suite sichert Portale von Banken, Versicherungen und Behörden und wird heute von Unternehmen weltweit eingesetzt. Sie schützt in der Schweiz über 80 Prozent aller E-Banking-Transaktionen und zahlreiche kritische E-Services weltweit. Auf der it-sa präsentiert das Unternehmen nevisDetect und eine neue Lösung für die mobile Authentisierung.

Von Stephan Schweizer, NEVIS Security GmbH

Es genügt längst nicht mehr, dass Unternehmen die Kundendaten schützen und gegen Diebstahl sichern, es ist inzwischen von zentraler Bedeutung, dass die Sicherheitsinfrastruktur feststellen kann, ob die Person, die sich online – egal von welchem Gerät – einloggt, auch wirklich der Nutzer ist, zu dem die Credentials gehören. Hierbei spielen zahlreiche Faktoren eine Rolle und nur eine durchgängige und auf verschiedene Authentisierungsmethoden zugeschnittene Lösung ist in der Lage, Abhilfe zu schaffen. Allerdings leiden bei vielen herkömmlichen Methoden das Bedienerlebnis und die Benutzerfreundlichkeit – niemand möchte im Urlaub automatisch aus seinen Accounts ausgesperrt werden, nur weil man sich aus einem anderen Land einloggt oder den Hardware-Token zu Hause vergessen hat. Die Balance zwischen Sicherheit und Einfachheit wird für viele Unternehmen zur Mammutaufgabe, bei der häufig an einem der beiden Enden gespart wird.

Die NEVIS Security GmbH ist auf der it-sa 2018 mit mehreren Neuheiten vertreten, die genau auf die veränderte Bedrohungslandschaft und die Kundenbedürfnisse zugeschnitten sind.

„Continuous Behaviour Analytics“

Inzwischen haben sich Online-Kriminelle bereits darauf eingestellt, dass sie beim Login in einen fremden Account Sicherheitsmaßnahmen umgehen müssen. Genau aus diesem Grund ist es wichtig, nicht nur den Login-Vorgang, sondern die gesamte Session kontinuierlich auf verdächtiges Verhalten zu untersuchen. Sich so vor Attacken zu schützen genießt höchste Priorität. Das gilt sowohl für Leistungsanbieter, die finanzielle Verluste und Reputationsschäden vermeiden wollen, als auch für Kunden, die ein Höchstmaß an Sicherheit erwarten.

Aktuell wurde eine neue Komponente zur Anomalie-Erkennung in die NEVIS Security Suite integriert, mit der „Continuous Behaviour Analytics“ – also Sicherheit durch durchgängige Mechanismen – ermöglicht wird. Diese hochsichere, aber gleichzeitig User-freundliche Komponente reiht sich als nevisDetect in die Security-Suite ein und wird auf der it-sa anhand von Live-Demos zu sehen sein.

Bei der Entwicklung der Komponente wurde beachtet, dass eine herkömmliche Zwei-Faktor-Authentisierung keinen ausreichenden Schutz mehr vor Identitätsdiebstahl oder Man-in-the-Browser-Angriffen bietet, die auf Schadprogrammen basieren. Hinzu kommt, dass eine Authentisierung mit mehreren Faktoren das Nutzererlebnis beeinträchtigt und so die Kundenbindung schwächt. Um die Sicherheit kritischer Dienste zu erhöhen, ohne Abstriche bei der Benutzerfreundlichkeit zu machen, sind deshalb neue, ganzheitliche Sicherheitskonzepte gefragt. Genau diese Anforderungen standen bei der Entwicklung von nevisDetect im Mittelpunkt. nevisDetect erkennt Verhaltensanomalien und berechnet für jede Benutzerinteraktion im Hintergrund einen Risikowert. Werden dabei gewisse Schwellwerte überschritten, so ist das System in der Lage, entsprechende Gegenmaßnahmen bis hin zum Session-Abbruch zu ergreifen.

Mobile Authentisierung

Ergänzend zur kontinuierlichen, verhaltensbasierten Authentisierung wird NEVIS auf der it-sa 2018 ihre neue Lösung für mobile Authentisierung einem breiten Publikum vorstellen. Jeder Mensch beschäftigt sich heute im Durchschnitt

mehr als drei Stunden täglich mit seinem mobilen Gerät. Egal, was verkauft oder gekauft werden möchte, es muss eine Möglichkeit bestehen, das einfach und sicher über ein mobiles Gerät erledigen zu können. Zudem wollen Kunden ihre Mobilgeräte zunehmend als primären oder sogar alleinigen Kanal für den Kontakt zu Unternehmen nutzen.

Technisch basiert die Mobile-Authentication-Lösung auf dem FIDO UAF-Standard. NEVIS unterstützt damit das Konzept „Mobile as a Token", bei dem das Mobilgerät als Speicherort von Schlüsselmaterial für die Authentisierung dient. Die neue Lösung erlaubt eine benutzerfreundliche starke Authentisierung auf dem Mobilgerät mit gängigen Mechanismen wie Fingerabdruckerkennung oder Face-ID. Die Authentisierung kann direkt in einer App (In-App) geschehen, oder auch für eine Webapplikation via Out-of-Band Push-Nachrichten. Auf dieselbe Weise lässt sich die Lösung auch für das Bestätigen von Transaktionen nutzen. Damit deckt die Mobile-Authentisierungs-Lösung zentrale Anwendungsfälle ab, wie sie für Angebote wie das Mobile-Banking gebraucht werden.

NEVIS MobiIe Authentication ist eine gute Ergänzung für die verhaltensbasierte, kontinuierliche Authentisierung. Einerseits ermöglicht sie eine benutzerfreundliche 2-Faktor-Authentisierung, andererseits kann sie aber auch im Verlauf der Session dazu benutzt werden, um Situationen mit erhöhtem Risiko aufzulösen, indem der Benutzer über einen separaten Kanal die Möglichkeit hat, seine Identität zu bestätigen.

Die Mobile-Authentication-Lösung erfüllt dabei höchste Ansprüche im Bereich Datenschutz und Sicherheit. So werden beispielsweise keinerlei biometrische Daten (Fingerabdruck etc.) an den Dienstanbieter übertragen, sämtliche Daten zur biometrischen Benutzererkennung verbleiben auf dem Gerät des Benutzers. Aufseiten des Dienstanbieters wird lediglich ein öffentlicher Schlüssel hinterlegt, mit dem sämtliche Interaktionen über kryptografische Mechanismen verifiziert werden können. Damit erfüllt die Lösung auch vollumfänglich die Anforderungen neuer Regulatorien, wie der DSGVO oder PSD2.

Die Bausteine „Mobile Authentication" und „Continuous Behaviour Analytics" bilden in Kombination mit klassischen Identity-Management-Funktionen ein umfassendes Customer-Identity-and-Access-Management-(CIAM)-System, das die effiziente, sichere und benutzerfreundliche Bewirtschaftung von digitalen Kunden-Identitäten ermöglicht.

CIAM-System

Die NEVIS Security Suite bietet neben der reinen sicheren Verwaltung von Identitäten und deren Authentifizierungsfaktoren auch eine Rundumsicht auf den Kunden. „Know your customer" dient als Basis für die Erstellung maßgeschneiderter Angebote und bildet somit die Grundlage für die Stärkung der Marktposition und der Kundenzufriedenheit jedes Unternehmens. Heute bedeutet ein solides CIAM-System nicht nur mehr Sicherheit, es spart durch höhere Benutzerfreundlichkeit auch Zeit und verringert Support-Anfragen. Damit wird es für jedes Unternehmen, das auf Nutzerkonten setzt, ein Muss. ■

Vorträge von NEVIS auf der it-sa

Dienstag, 09.10.2018, 11:00 bis 11:15 Uhr, M10 – Management Forum in Halle 10.1
Digitale Transformation – Business-Disruptor oder kalter Kaffee?
Stephan Schweizer, Chief Product Officer (CPO) – AdNovum Informatik AG

Dienstag, 09.10.2018, 15:30 bis 15:45 Uhr, T10 – Technology Forum in Halle 10.0
AdNovum – Live-Hacking: Cybercrime in der Realität – ist Ihr Unternehmen „richtig" geschützt?
Konstantin Luttenberger, Pre-Sales – AdNovum Informatik AG

Dienstag, 09.10.2018, 16:30 bis 16:45 Uhr, NEVIS-Stand
Live-Hacking-Demo
Konstantin Luttenberger, Pre-Sales – AdNovum Informatik AG
anschließend: Apéro/Umtrunk

Mittwoch, 10.10.2018, Congress@it-sa im NCC Mitte
Kongress FSP – Präsentationen von NEVIS, Partnern und Kunden

Messestand: Halle 10.0, Stand 10.0-316