LANline

10,– €

Juli 2018
26. Juni

IT ■ Network ■ Datacenter www.lanline.de

Datacenter Security und Hochverfügbarkeit

Normen im Blick: EN 50600 und Co.

Schutz mittels Hypervisor

Aktuelle USV-Technik

Mit Marktübersicht Kühlsysteme

Neue Serie zur OT-Sicherheit
Kooperation von IT und Produktion

Administrations-Tools unter der Lupe
Windows Admin Center und Icinga 2 im Praxistest

Sonderdruck AdNovum
Mit Intelligenz gegen Identitätsdiebstahl

Kontextabhängige Authentisierung

Mit Intelligenz gegen Identitätsdiebstahl

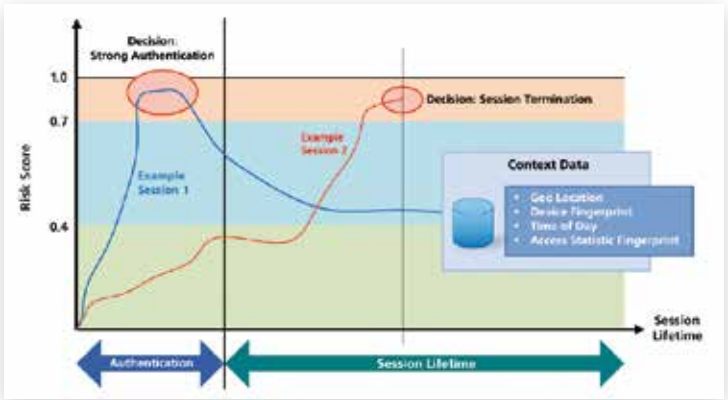
Möglichst bequem oder so sicher, wie es nur geht? Die aktuelle Bedrohungslage verschärft den klassischen Konflikt zwischen den Fürsprechern möglichst benutzerfreundlicher Online-Authentisierungsmethoden und den Vertretern des Sicherheitslagers, das den optimalen Schutz der Anwenderdaten fordert. Kontextabhängige Authentisierung wird beiden Seiten gerecht.

Es liegt in der Natur der Sache, dass das Identitäts-Management in Unternehmen immer wieder den Widerspruch zwischen Sicherheits- und Bequemlichkeitsaspekten provoziert. Während die Existenz von Firewalls, Virenschutz und Security-Intelligence-Lösungen nur im Fall einer aktuellen Bedrohung spürbar wird, können Authentisierungssysteme so gut wie nie unmerklich im Hintergrund laufen: Der Anmeldevorgang an einem Computersystem erfordert in jedem Fall eine Interaktion mit dem Anwender. So setzt sich die Authentisierungsmethodik immer wieder der Beurteilung durch die Nutzer aus. Empfinden die Anwender konkrete Anmeldeschritte als zu umständlich und stehen ihnen zugleich attraktivere Alternativen zur Verfügung, wenden sie sich ab.

Gleichzeitig sind Online-Anbieter und Betreiber unternehmensinterner Authentisierungssysteme gezwungen, das Sicherheitsniveau eher zu heben als zu senken. Denn Identitätsdiebstahl ist eines der Hauptbetätigungsfelder der Cyberkriminellen. Spezialisierte Banden greifen Daten in Massen ab und verkaufen sie dann weiter – und kleine, hochprofessionelle Teams fischen nach den Anmeldeinformationen privilegierter Nutzer, um deren Identitäten für gezielte Angriffe auf besonders lohnenswerte Informationsbestände zu nutzen.

Massendiebstähle gehen meist mit Angriffen auf Datenbanken einher. Doch wenn Angreifer den wahrscheinlichen Erlös aus dem Missbrauch bestimmter Identitäten gut berechnen können, lohnen sich für sie auch Angriffe auf Endgeräte, bestimmte Kommunikationsverbindungen oder das Lauschen auf den Beginn typischer Transaktionen – etwa Online-Banking aus einen großen Hotel heraus.

Vor allem bei sensiblen Daten, wie sie zum Beispiel beim Online-Banking und im Gesundheitswesen im Spiel sind, können die resultierenden Schäden für Privatpersonen und die Anbieter der genutzten Dienste immens sein. Aus diesem Grund stellt auch die neue EU-Datengrundschutzverordnung (DSGVO) hohe Anforderungen an den zweckgebundenen Umgang mit Kundendaten und -identitäten und verlangt einen noch besseren Schutz.



Die kontinuierliche risikobasierte Benutzerauthentisierung korreliert die Ausgaben mehrerer Anomalieerkennungsmodule. Bild: AdNovum

Komfort vs. Schutz

Bisher galten die Kennwort-Authentisierung mit erzwungenermaßen hoher Passwortsicherheit und die Zwei-Faktor-Authentisierung (2FA) als die gängigsten Antworten auf die Bedrohungslage und Compliance-Anforderungen. Für kritische Systeme reicht mitunter inzwischen aber beides nicht mehr aus. Angreifer schaffen es, neben Benutzername/Passwort-Kombinationen bei hinreichender Motivation auch den zweiten Faktor an sich zu bringen, um nicht-autorisierten Zugriff auf Anwendungen zu erlangen. Da sich der Angreifer dann mit den Zugangsdaten eines autorisierten Benutzers einloggen kann, hat das Authentisierungssystem kaum eine Chance, den bösartigen Charakter des Zugriffsversuchs zu erkennen.

Vor diesem Hintergrund könnte man auf noch stärkere Authentisierungsmethoden setzen, also beispielsweise auf Drei-Faktor-Methoden mit einer zusätzlichen Biometrieauswertung. Doch dies könnte im Einzelfall die Anwender nicht nur abschrecken, sondern auch verunsichern und die Akzeptanz von Online-Services grundsätzlich beeinträchtigen.

Verhaltensanalyse

Ein besserer Ansatz ist die kontextabhängige Authentisierung. In der reaktiven Sicherheitstechnik, also beim Einsatz von Angriffserkennungssystemen wie SIEM-Produkten (Security-Information- und Event-Management) oder Systemen zur Netzwerk-Verhaltensanalyse, ist die Fähigkeit zum kontextabhängigen Vorgehen längst ein Qualitätsmerkmal. Die hier eingesetzten Werkzeuge suchen nach An-

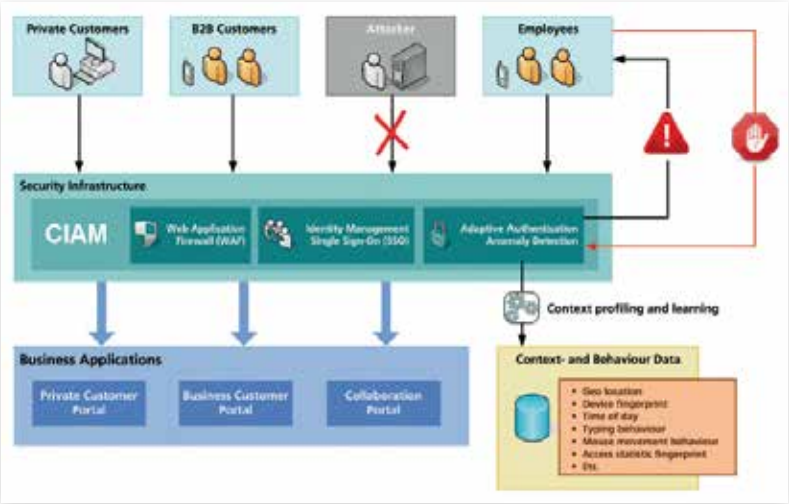
omalien im Kommunikationsgeschehen; diese setzen sie dann beispielsweise mit Informationen über den Wert der Systeme und Informationen in Beziehung, die möglicherweise betroffen sind. Daraus ergeben sich automatisch ermittelte Risikobewertungen, die einen direkten Einfluss auf die Reaktionen der Sicherheitssysteme haben. Diese reichen von der stillschweigenden Weitergabe der Erkenntnisse an Analystenteams bei weniger relevanten Vorfällen bis – im Extremfall – zum vollen Alarm mit sofortiger Beendigung der Session.

Kontextabhängige Authentisierung trägt diese Flexibilität und Anpassungsfähigkeit auch in die Prävention. Ein CIAM-System (Consumer-Identity- und -Access-Management) zum Beispiel, das auf eine derartige Technik setzt, versucht schon bei der Einleitung eines Anmeldevorgangs und während der dann laufenden Sitzung stets zu berücksichtigen, was geschehen soll und unter welchen Umgebungsbedingungen die Aktivität stattfindet. Denn Angreifer müssen gestohlene digitale Identitäten irgendwann einsetzen – doch das werden sie nur selten in einer Weise tun können, die exakt dem Vorgehen des normalen Benutzers entspricht.

Zu den möglicherweise relevanten Kontextinformationen, deren Auswertung sich lohnt, zählen:

– Feststellung, ob das zur Anmeldung genutzte Gerät bekannt oder unbekannt ist,
– Zugriffszeit,
– Geolokation (Zugriff von einem ungewöhnlichen Standort aus),
– physisch unmöglicher Ortswechsel zwischen zwei Anmeldevorgängen,
– vertrautes oder stark abweichendes Verhalten beim Tippen oder bei der Maus-/Touchscreen-Bedienung,
– Art und Wert der angeforderten Transaktion und
– Gerätewechsel innerhalb derselben Sitzung.

Ein CIAM-System, das über die entsprechenden Funktionen verfügt, kann die oben gelisteten Informationen und weitere Daten für eine Risikobewertung heranziehen, die es auch im Verlauf der weiteren Schritte des Nutzers stetig aktualisiert. Erreicht der Risikowert einen vorher definierten Schwellenwert, kann das System automatisch reagieren – etwa mit der Forderung nach einer weiteren Authentisierung oder einer zusätzlichen Bestätigung, die vor einer Aktion wie dem Anstoßen einer Überweisung im Zahlungsverkehr fällig wird. Auch ein Verbindungsabbruch und eine Warnung an den Service-Provider lassen sich bei extremer Auffälligkeit auslösen. Zugleich kann ein solches System aber auch auf eine starke Anmeldesicherung verzichten, wenn der Kontext auf geringe Gefahren schließen lässt. Dies erhöht dann den Komfort für den Nutzer.



Die zwischengelagerte Security-Infrastruktur eines CIAMs sichert den Zugang, autorisiert den Anwender und kann auch eine Anomalieerkennung implementierten.

Bild: AdNovum

Die verwendeten Informationen sind teils generisch, etwa Geolokationsdaten, basieren aber mitunter auch auf längerfristig ermittelten Nutzerprofilen. So fallen Ortswechsel bei einem Anwender, der häufig in ganz Europa oder gar weltweit unterwegs ist, weniger stark als Risikoindikator ins Gewicht als bei einem Nutzer, der gewöhnlich immer am selben Ort operiert. Aus Datenschutzgründen muss ein Anwender diesen Verfahren gegebenenfalls zustimmen. Allerdings ist dabei zu bedenken, dass gerade im Bankbereich schon länger Fraud-Detection-Systeme mit Anomalie-Erkennungskomponenten zum Einsatz kommen, da für Banken entsprechende gesetzliche Verpflichtungen bestehen.

Compliance-Anforderungen

Wie bei allen intelligenten Sicherheitssystemen gibt es Voraussetzungen für das optimale Funktionieren kontextgestützter Authentisierung: Der Betreiber muss sich zuvor mit den Bedrohungsszenarien in seinem Geschäftszweig befasst haben; zudem müssen die Schwellenwerte für die Bewertungsparameter der Anmeldevorgänge nach sinnvollen Risikowerten modelliert sein. Entsprechende Assessments sind speziell in der Finanzbranche ohnehin vorgeschrieben. Nebenher sorgen sie dafür, dass die Konfiguration eines CIAMs, das Kontextinformationen nutzt, auch externen Audits standhält.

Wie aufwendig das Einpflegen von Schwellenwerten ist, hängt von Einsatzszenario ab: Generelle Festlegungen wie der Risikowert von Zugriffen aus bestimmten Ländern oder vom bekannten eigenen PC im Vergleich zu Fremdgeräten sind eher einfach umzusetzen und können über längere Zeiträume statisch sein. Individuellere Bedingungen hingegen erfordern eventuell echte Assessments und eine dynamische Kopplung an externe Security-Intelligence-Informationen.

Die Gefahr, Nutzer durch sich gelegentlich ändernde Sicherheitsanforderungen bei Anmeldungen zu irritieren, ist gering. Es mag zwar stimmen, dass Menschen generell Probleme mit Risikoeinschätzungen haben und dass dies vor allem im Online-Verhalten Wirkung zeigt, aber die schnelle, effektive Anpassung des eigenen Verhaltens an eine erkannte Gefahrenlage gelingt ihnen gewöhnlich sehr gut.

Stephan Schweizer/wg

Stephan Schweizer ist CPO für Nevis bei AdNovum, www.nevis-security.ch.