Sicher mit der Digitalisierung gehen

Die Digitalisierung ist im Mittelstand angekommen. Kaum ein Unternehmen kommt mehr ohne die Cloud aus. Mitarbeiter haben mit BYOD („Bring your own device" = private mobile Endgeräte) von überall aus Zugriff auf alle Daten. Zahlreiche weitere Web-Anwendungen erleichtern und verändern den Arbeitsalltag. Unternehmen, die noch nicht auf den Zug der Digitalisierung aufgesprungen sind, sollten sich beeilen, aber in der Umstellung auch die damit verbundenen Sicherheitsrisiken berücksichtigen. Die digitale Transformation sollte immer auch IT-Security-Lösungen zum Schutz von Daten, Identitäten und Applikationen umfassen.

Die Vorteile der Digitalisierung liegen auf der Hand: Sie ermöglicht die Erweiterung des Geschäftsfeldes, das nun nicht mehr geografischen Grenzen unterliegt. Theoretisch kann jedes Unternehmen deutschlandweit oder sogar weltweit ohne großen Mehraufwand tätig werden. Ein weiterer Vorteil ist die Optimierung und Beschleunigung der Geschäftsprozesse. Effizienz und Produktivität können drastisch gesteigert werden, und durch eine geschickte Digitalisierungsstrategie können Sie sich beachtliche Wettbewerbsvorteile sichern, Kosten senken und Umsätze steigern.

Web-Anwendungen sind bei der Digitalisierung von Geschäftsprozessen meist der Dreh- und Angelpunkt, wenn es um die Interaktion mit Menschen geht. Ein externer Zugriff auf den internen Sharepoint oder Exchange ermöglicht den Mitarbeitern etwa ein Arbeiten von überall zu jederzeit wie im Büro. Auch Cloud-Lösungen wie Office 365 oder Salesforce sowie viele selbstentwickelte Fachapplikationen sind als Web-Anwendungen umgesetzt.

Die Anwendungsbeispiele für erfolgreiche Digitalisierung sind zahlreich. Das digitale Banking war nur der Vorreiter. E-Government, E-Health oder Industrie 4.0 sind weitere Bereiche. Durch moderne ERP-Systeme (Enterprise-Resource-Planning) wie SAP oder Oracle können Lieferanten direkt auf Systemteilbereiche zugreifen, und verschiedene Firmenniederlassungen werden direkt miteinander verbunden, um Produktionsprozesse und Warenbestellungen zu automatisieren und zu optimieren. Maschinen beginnen direkt miteinander zu kommunizieren. Auch dieser Kommunikationskanal wird immer häufiger mittels so genannter Werbservices von außen zugänglich gemacht.

© MARTIN BURKHART

*Ihr Experte: **Martin Burkhart** ist Product Manager Web Application Security bei Ergon Informatik AG*

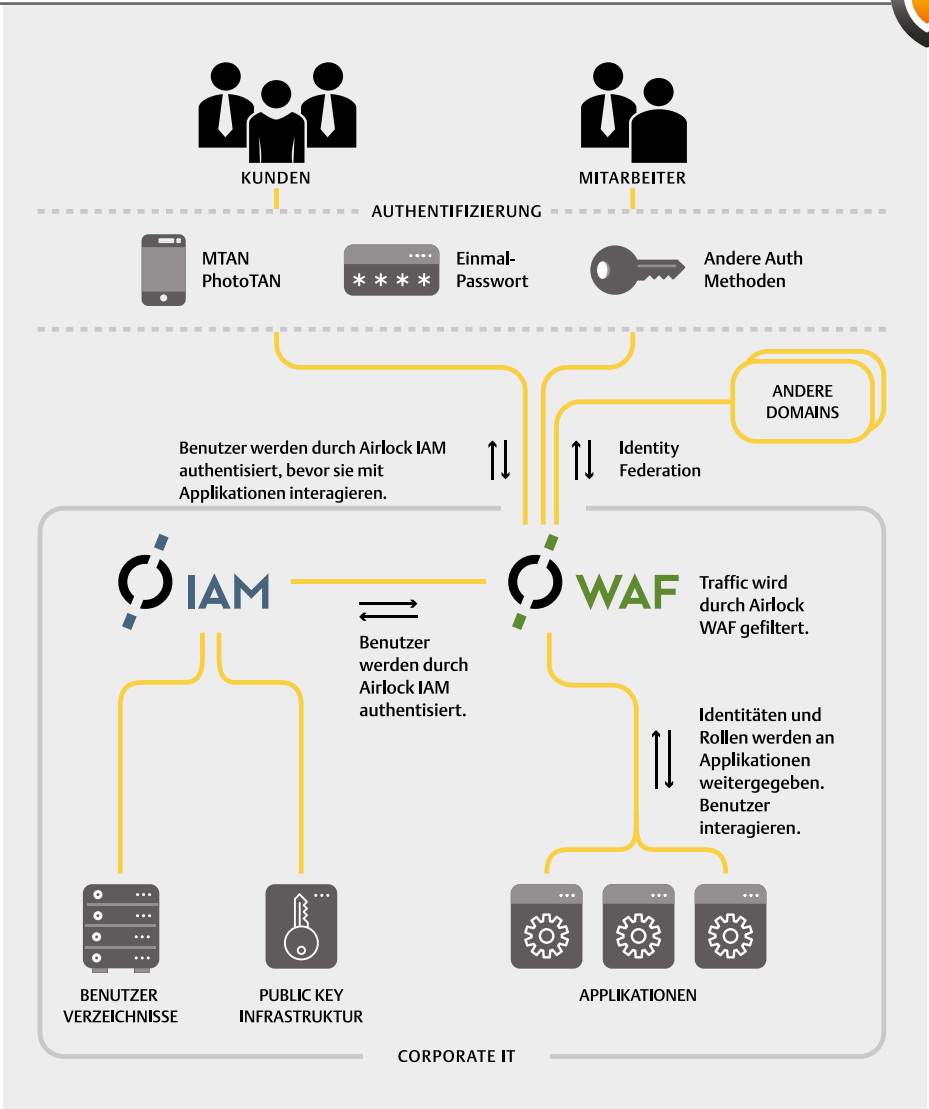
Angriffspunkt: Web-Anwendungen

Dem deutschen Mittelstand sind jedoch die Gefahren selten bewusst, die durch die Einbindung von Web-Anwendungen entstehen. Klassische Netzwerk-Firewalls schützen nicht gegen Angriffe auf Applikationsebene und oft erhalten schlecht geprüfte Identitäten Zugriff auf sensitive Daten. Die häufig eingesetzten traditionellen Virenschutz- und Firewall-Lösungen greifen hier nicht. Dabei sind 75 % aller Web-Anwendungen verwundbar und damit einer potenziellen Gefährdung ausgesetzt.

Diese Unwissenheit kann den Mittelstand teuer zu stehen kommen. Industriespionage von Mitbewerbern ist das heikelste Thema. Hacker aus dem Ausland, wie etwa aus China oder Russland, lassen sich für wenig Geld anheuern und nutzen genau diese Schwachstellen aus. Sie erbeuten dabei häufig Anmeldedaten für Benutzerkonten, die dann auf dem Schwarzmarkt gehandelt oder öffentlich ins Netz gestellt werden. Dies führt zu negativer Berichterstattung in den Medien und das kann die Reputation eines Unternehmens in Mitleidenschaft ziehen. Sind von einem Hack Produktionsanlagen betroffen, steht meist einmal alles still, solange die Schäden im IT-System noch nicht behoben sind. Das führt zu starken Umsatzeinbußen.

Gravierende Auswirkungen auf ungesicherte Unternehmen

Das Open Web Application Security Project (OWASP) ist eine offene Community mit dem Ziel, Organisationen und Unternehmen bei der Verbesserung der Sicherheit von Web-Anwendungen zu unterstützen. Die OWASP Top 10 geben einen Überblick über die 10 wichtigsten Schwachstellen und Sicherheitsrisiken für Web-Anwendungen (s. *www.owasp.org/index.php/Category:OWASP_Top_Ten_Project*).



Authentifizierung: Authentifizierungsplattform und Web Application Firewall

Laut OWASP können die Folgen ungesicherter Web-Applikationen gravierend sein, die Liste ist lang:

- Ein Angreifer kann Eingabedaten so manipulieren, dass er nicht vorgesehene Kommandos ausführen oder unautorisiert auf Daten zugreifen kann.
- Angreifer können die Identität anderer Benutzer annehmen.
- Sie können Benutzersitzungen übernehmen, Seiteninhalte verändern oder den Benutzer auf bösartige Seiten umleiten.
- Sie erlangen unautorisiert Zugriff auf Daten.
- Angreifer können geschützte Daten (wie Kreditkartendaten oder Zugangsinformationen) auslesen, modifizieren und mit ihnen weitere Straftaten wie beispielsweise Kreditkartenbetrug oder Identitätsdiebstahl begehen.
- Angreifer können Aktionen innerhalb der betroffenen Anwendungen im Namen und Kontext des angegriffenen Benutzers ausführen.
- Ein Angriff kann zu schwerwiegendem Datenverlust bis hin zu einer Serverübernahme führen.
- Angreifer können ihre Opfer auf Phishing-Seiten oder Seiten mit Schadcode um- oder weiterleiten.

Diese Bedrohungen sind nicht nur komplex, sondern können Unternehmen bis in ihre Existenzgrundlage erschüttern. Daher ist es von enormer Wichtigkeit, Web-Anwendungen zu schützen. Dafür sorgen so genannte Web Application Firewalls (WAF), die diese Gefahren abwehren. Sie kontrollieren den Inhalt aller gestellten Anfragen und lassen Gefährdungen nicht durch.

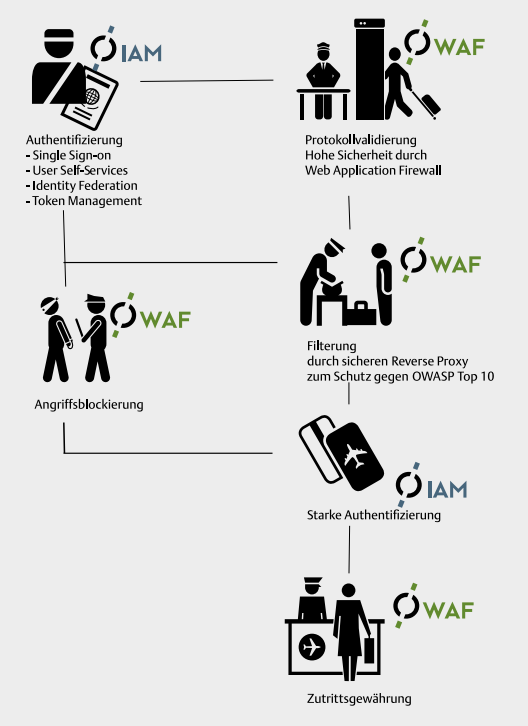
Da eine WAF den Applikationen vorgelagert ist, sind alle Applikationen dahinter sicher: Sie können auch bequem neue Anwendungen hinzufügen und die Web Application Firewall schützt sie automatisch mit. Die Sicherheit der Applikationen und Daten wird jedoch erst ausreichend, wenn nicht nur der Inhalt der Anfragen geprüft wird, sondern auch die Identität der Anfragensteller. Das erledigt eine Authentifizierungsplattform. Erst die kombinierte Anwendung der 2 Tools nimmt Angreifern den Wind aus den Segeln.

Sicherheit wie am Flughafen

Die Situation lässt sich mit der Kontrolle am Flughafen vergleichen: Die Passkontrolle sowie der Gepäck- und Personenscan schützen vor vielen Gefahren, die sonst mitfliegen würden. Das Sicherheitspersonal hält gefährliche Kofferinhalte oder Personen davon ab, in ein Flugzeug zu gelangen. Dabei helfen ihnen festgelegte Sicherheitsabläufe und Tickets. Ohne diese wäre das Fliegen eine sehr chaotische und unsichere Angelegenheit. Dasselbe gilt für den Digitalisierungsprozess.

Die vorgelagerte Kombination aus Authentifizierungsplattform und Web Application Firewall schützt Ihre Anwendungen vor den OWASP Top 10 Bedrohungen. Außerdem amortisieren sich die Aufwände mit jeder weiteren Applikation, die angeschlossen wird. Statt ein separates Passwort für jede

Anwendung zu vergeben, können die Applikationen bequem im bestehenden Single Sign-on (SSO) Verbund integriert werden. Der kombinierte Schutz ermöglicht außerdem die Verteilung verschiedener Rollen, die mit entsprechenden Zugriffsrechten ausgestattet sind. So können unbekannte Identitäten beispielsweise nur die öffentliche Webseite ansehen. Lieferanten hingegen können auf alle für sie relevanten Daten zugreifen, während Sie Mitarbeitern umfassenden Zugriff gewähren können.



Sicherheitsabläufe wie am Flughafen

Die Web Application Firewall Airlock WAF und Authentifizierungsplattformen Airlock IAM erhalten Sie bei ausgewählten Systemintegratoren wie secunet Security Networks AG, Thinking Objects, cirosec oder SHE Informationstechnologie AG. Sie installieren und betreuen die Lösungen in Ihrem Unternehmen. Die Kosten für eine solche Lösung variieren abhängig von der Anzahl der zu schützenden Anwendungen und Benutzer.

Fazit

Die Digitalisierung bringt nicht nur zahlreiche Vorteile mit sich, sondern setzt sensitive Unternehmensdaten zusätzlichen Schwachstellen aus, da Web-Anwendungen auf verschiedenen Ebenen angreifbar sind. Der traditionelle Anti-Viren-Schutz und die klassische Netzwerk-Firewall arbeiten auf einem anderen Layer und können Sie vor diesen Bedrohungen nicht schützen. Daher benötigen Sie eine Web Application Firewall, welche die verwendeten Web-Protokolle versteht und entsprechende Angriffe präventiv blockieren kann. Den besten Schutz erhält man in Kombination mit einer vorgelagerten Authentifizierungsplattform, welche sicherstellt, dass Zugriffe sicher authentifiziert und autorisiert werden. □

Checkliste für eine erfolgreiche und sichere Digitalisierung	
Optimierung: Überlegen Sie, wo die Digitalisierung Kosten spart und Umsätze steigert.	☐
Immer aktuell: Web-Applikationen sollten auf dem neuesten Stand der Technik entwickelt sein und durch Updates aktuell gehalten werden.	☐
Der Kunde ist König: Einfachheit und Benutzerfreundlichkeit sollten in der Anwendung im Vordergrund stehen. Denken Sie sich in die Rolle des Anwenders der Applikation.	☐
Verfügbarkeit: Sie müssen gewährleisten, dass die Anwendungen jederzeit verfügbar sind. Schließlich sind die meisten Applikationen geschäftskritisch und deren Ausfälle wirken sich direkt auf Umsatz und Kosten aus.	☐
Zentral und vorgelagert: Die Sicherheit der Applikationen sollten Sie über eine Web Application Firewall zentral und vorgelagert gewährleisten. Klassische Firewalls können hier keinen Schutz bieten. Tauchen Sicherheitsschwachstellen in Protokollen oder Frameworks auf, können Maßnahmen unmittelbar vorgelagert und über alle Anwendungen hinweg getroffen werden.	☐
Single Sign-on: Prüfen Sie die Möglichkeit eines Single Sign-ons (SSO) auf Ihre gesamte Service-Palette. Dies vereinfacht nicht nur die Entwicklung von Applikationen, sondern auch den Roll-out und den Support. Zudem erhöht es die Benutzerfreundlichkeit und letztlich auch die Sicherheit Ihrer Applikationen.	☐
Rollenverteilung: Prüfen Sie Zugriffsrechte (wer darf auf welche Applikation zugreifen) in der vorgelagerten Lösung. Das entlastet die Anwendungen und vereinfacht die Nutzung eines einzigen Benutzerkontos (Single Sign-on).	☐
Gesetzesanforderungen: Bedenken Sie im Digitalisierungsprozess eventuelle Gesetzesanforderungen (z. B. Datenschutzgesetz, EBA-Anforderung, PCD-DSS, IT-Sicherheitsgesetz). Ist für die Benutzeranmeldung eine starke Authentifizierung erforderlich? Müssen die Daten verschlüsselt übertragen werden?	☐
Schutz der Daten: Sensible Daten sind das Herzstück der Digitalisierung – schützen Sie sie entsprechend. Sie sind das neue Gold.	☐
Notfallplan: Sie sollten einen Notfallplan entwickeln, um in kürzester Zeit auf Abfluss sensibler Daten, digitale Wirtschaftsspionage oder Sabotage reagieren zu können.	☐