

Network Access Control: Wesentlicher Bestandteil für die IT-Sicherheit kritischer Infrastrukturen

Banken, Kreditinstitute, Finanzdienstleister und Versicherungsunternehmen gehören zu den Institutionen mit den höchsten Anforderungen an die Informationssicherheit. Dies liegt zum einen daran, dass nahezu alle Geschäftsprozesse IT-gestützt sind, zum anderen steigen die Bedrohungen durch die Cyber-Kriminalität erheblich. Diese wachsende Verwundbarkeit und Gefahr wirtschaftlicher Schäden in Folge von IT-Risiken erhöht den Handlungsdruck für ein aktives IT-Sicherheitsmanagement im Finanz- und Versicherungswesen.



Einhaltung gesetzlicher Vorgaben und Bestimmungen

Der Gesetzgeber berücksichtigt die ansteigenden Bedrohungen im Bereich der Informationstechnologie und es gibt eine Reihe von Regularien und gesetzlichen Auflagen zur Risikominimierung. So definiert das in 2015 verabschiedete IT-Sicherheitsgesetz (ITSiG) in Deutschland Banken, Kreditinstitute, Börsen, Finanzdienstleister und Versicherungen als Betreiber Kritischer Infrastrukturen (KRITIS) und sieht Mindeststandards bei der IT-Sicherheit vor. Zeitnah folgt die europäische Richtlinie zur Netz- und Informationssicherheit (NIS), die zusätzliche Maßnahmen von Unternehmen und der gesamten öffentlichen Verwaltung fordern wird.

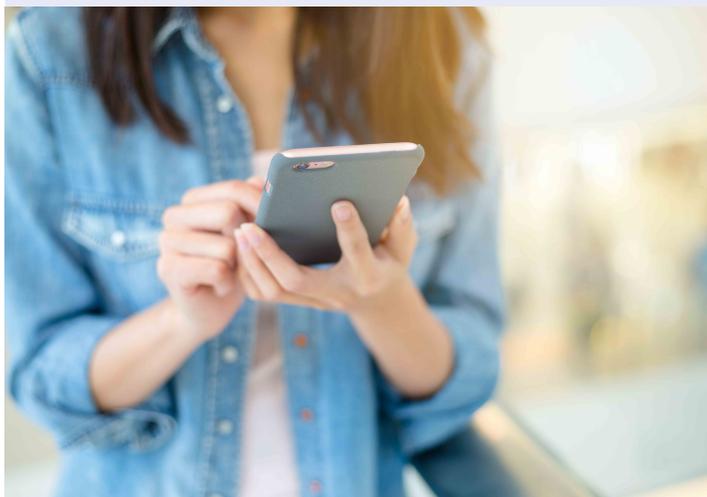
Die von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) herausgegebenen Mindestanforderungen an das Risikomanagement (MaRisk) fordern „für die IT-Systeme und die zugehörigen IT-Prozesse die Sicherstellung der Integrität, der Verfügbarkeit, der Authentizität sowie der Vertraulichkeit der Daten.“ Es wird empfohlen, bei der Ausgestaltung der Sicherheit der IT-Systeme und der zugehörigen IT-Prozesse grundsätzlich auf gängige Standards wie die IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnologie (BSI) oder die entsprechende ISO-Norm 27001 und 27002 zu setzen.

macmon-Nutzen für den Netzwerkschutz im Finanzwesen

- ✓ Überwachung und Kontrolle aller im Netzwerk befindlichen Geräte (Live-Bestandsmanagement) und Dokumentation aller Netzwerkzugriffe.
- ✓ Sicherstellung der Integrität des Netzwerkes durch ausschließliches Gewähren des Netzwerkzugangs für die definierten (eigenen und zugelassenen) Geräte.
- ✓ Ermöglichung des zeitlich und räumlich flexiblen Zugriffs auf ausgewählte Netzwerkbereiche (VLANs, WLANs) und sensible Daten bei gleichzeitigem Schutz vor unbefugtem Zugriff.
- ✓ Unterstützung bei der Umsetzung der vom BaFin herausgegebenen Mindestanforderungen an das Risikomanagement (MaRisk) und der Zertifizierung nach ISO 27001/27002.
- ✓ Unterstützung bei der Umsetzung der BSI-Standards zum Informationssicherheitsmanagement, der IT-Grundschutz-Kataloge und der Mindeststandards nach dem ITSiG.

In diesen Standards finden sich eine Vielzahl von Empfehlungen zur Netzwerksicherheit. So muss „die Installation und Benutzung nicht freigegebener IT-Komponenten verboten und die Einhaltung dieses Verbotes regelmäßig kontrolliert werden.“ (BSI M 2.216). Das Einbringen von nicht autorisierten und unsicheren Geräten ins Netz ist konsequent zu unterbinden.

Die von macmon secure entwickelte NAC-Lösung macmon gewährleistet die Einhaltung dieser Sicherheitsregularien.



Netzwerkübersicht und Datenschutz

Mit macmon NAC wissen Sie jederzeit, welche Geräte sich in Ihrem Netzwerk befinden und können Ihre eingesetzten PCs, Drucker, Laptops und technischen Geräte jederzeit effizient überwachen. macmon erkennt, meldet und unterbindet den Betrieb von Fremdsystemen im Netzwerk und verhindert den Einsatz von nicht autorisierten Geräten. Als herstellerunabhängige Sicherheitslösung bietet macmon eine verlässliche Überwachung auch von Netzen mit unterschiedlichsten Netzwerkkomponenten und ist in der Lage auch für Spezial-Geräte, wie z. B. Geldautomaten mit Netzwerkzugriff in öffentlichen Bereichen, eine verlässliche Geräteerkennung durchzuführen.

macmon bietet eine flexible Lösung, die auch einen erweiterten Mischbetrieb mit SNMP und 802.1X unterstützt. Gast- und Mitarbeitergeräte (BYOD) können außerdem über das Gästportal, mithilfe eines dynamischen Managements der Netzwerksegmente, einfach und sicher zugelassen werden.

Kontakt

macmon secure GmbH
Alte Jakobstraße 79-80 | 10179 Berlin
Tel.: +49 30 2325777-0 | nac@macmon.eu | www.macmon.eu

Der Datenschutz und der verantwortungsvolle Umgang mit vertraulichen Daten hat im Finanz- und Versicherungswesen eine besonders hohe Bedeutung. Die Kundensetzen voraus, dass der Schutz persönlicher Daten stets gewahrt wird. Die unerwünschte Offenbarung vertraulicher Kunden- oder Konten-Daten stellt somit ein erhebliches Risiko dar. Die rechtlichen Folgen reichen bis zur persönlichen Haftung der Vorstände, welche nach § 91 Abs.2 AktG geregelt ist.

macmon sorgt dafür, dass sich nur autorisierte, authentifizierte und sicher konfigurierte Systeme im Netz befinden. Somit hilft macmon, ein Eindringen in die Informationssysteme zu verhindern und sensible Daten und personenbezogene Informationen abzusichern und vor unberechtigten Zugriffen zu schützen. Bei auffälligem Verhalten von Endgeräten oder manipulierten Unternehmensgeräten von denen möglicherweise ein unerlaubter Zugriff auf bspw. Kreditkartendaten erfolgt, trennt macmon diese vom Produktivnetzwerk, so dass keine weitere Bedrohung mehr von diesen ausgehen kann.

macmon NAC: Geprüfte Sicherheit nach Common Criteria

Bestandteil der Cyber-Sicherheitsstrategie der Bundesregierung ist die Förderung und Forderung des Einsatzes von IT-Komponenten, die sich „einer Zertifizierung nach einem international anerkannten Zertifizierungsstandard unterzogen haben“. Das BSI hat der macmon secure GmbH für Ihre Network-Access-Control-Lösung macmon NAC ein BSI-Zertifikat (Zertifizierungskennnummer BSI-DSZ-CC-0738-2015) nach den weltweit gültigen Anforderungen der Common Criteria (CC) ausgestellt.

Damit bietet macmon secure eine NAC-Lösung an, die den eigenen NAC-spezifischen Sicherheitsvorgaben und allgemein anerkannten Sicherheitskriterien entspricht. Eine detaillierte Beschreibung der Sicherheitsleistung der zertifizierten NAC-Version kann im Zertifizierungsreport unter www.macmon.eu/bsi-cc nachgelesen werden.