Informationssicherheit

Netzwerk

Regelung Nr. 03.02.04

Netzwerkzugänge

Klassifikation: Intern – KSU 2.1

Geltungsbereich: Die Regelungen gelten für die AUDI BRUSSELS

Version 1.0

Inhalt

I. Zweck

Der Zweck dieser Regelung ist die Definition von Sicherheitsanforderungen für:

- Content Filtering, wenn mit dem Internet kommuniziert wird
- Remote Access
- Sicherheitsanforderungen zur Anbindung von neuen Gesellschaften oder Partnerfirmen

Im Sinne dieser Regelung bedeutet der Begriff „Informationssicherheit“ IT-Sicherheit als Bestandteil einer ganzheitlichen Informationssicherheit.

1. Content Filtering

1.1. Übersicht

Die folgenden Protokolle erfordern zusätzliche Überprüfungen, um bösartige Daten bzw. Daten, die nicht im Interesse der Gesellschaft sind, zu blockieren oder zu löschen:

- HTTP(S) (Webbrowser und Webservices)
- (S)FTP (Dateiübertragung)
- SMTP (E-Mail)

Anforderungen sind in den folgenden Kapiteln beschrieben.

1.2. Validierung der Datenübertragung durch HTTP(S) und (S)FTP

1.2.1 Übersicht

Während des Datenaustauschs über HTTP(S) oder FTP, SFTP und denen, die über SSL gesichert sind, existieren die folgenden Risiken:

- Übertragung von Malware, Trojanern und anderem bösartigen Code
- Herunterladen und Ausführen von aktiven Inhalten, die beispielsweise bösartigen Code enthalten
- Zugriff auf Websites mit Inhalten, die nicht im Interesse des Unternehmens sind oder sogar gegen das Gesetz verstoßen
- Abfluss nicht öffentlicher Informationen des Unternehmens in Richtung des Internets

1.2.2 Schutz vor bösartigem Code

Jeglicher eingehende und ausgehende Datenverkehr muss auf bösartigen oder unerwünschten Code (z. B. Malware, Trojaner, Dialer, bösartigen Code in ActiveX, Java oder JavaScript) gescannt werden. Identifizierter bösartiger Code muss gelöscht werden.

1.2.3 URL-Filterung

URL-Filterung muss implementiert werden, um Zugriff aus dem Konzernnetzwerk auf Seiten mit ungesetzlichen Inhalten[1] zu verhindern.

Ein Programm zur Überwachung des Internetzugriffs (Inhaltsfilter-Software) anhand einer Prüfliste[2] kann zu diesem Zweck implementiert werden:

- Es sollte möglich sein, die Internetadressen in der Prüfliste in vordefinierte Kategorien (z. B. Malware verteilende Seiten, filesharing Plattformen, …) zu unterteilen. Ist eine Kategorie blockiert, dürfen Benutzer nicht auf Internetseiten mit URLs oder IP-Adressen dieser Kategorie zugreifen können.
- Ist der Zugriff auf eine notwendige Internetseite nicht möglich, da die entsprechende URL oder IP-Adresse zu einer blockierten Kategorie gehört, muss es möglich sein, diese Seite der Whitelist[3] hinzuzufügen.
- Die Prüfliste muss regelmäßig aktualisiert werden.

1.3. Validierung der Datenübertragung über SMTP

1.3.1 Übersicht

Beim Empfangen oder Senden von E-Mails über das Internet bestehen folgende Risiken:

- Übertragung von Viren, Trojanern und anderen bösartigen Programmen
- Produktivitätsverlust und rechtliche Probleme durch nicht angeforderte Massen- oder Junk-E-Mails (sogenannten SPAM E-Mails)
- Empfang von Phishing-E-Mails, welche Empfänger zu unerwünschten Handlungen verführen sollen (z.B. CEO Fraud)

1.3.2 Schutz vor bösartigem Code (SMTP)

Jeglicher ein- oder ausgehende E-Mail-Verkehr muss auf bösartigen Code überprüft werden.

Verschlüsselte Daten müssen am Gateway analysiert werden. Ist dies nicht möglich, müssen geeignete Schutzprogramme auf internen Systemen installiert werden, damit die Validierung direkt nach der Inhaltsentschlüsselung gewährleistet ist.

Die Regelung 03.01.01 Anti Malware und Systemschutz[4] muss beachtet werden.

1.3.3 Blockierung bestimmter Dateitypen (SMTP)

E-Mail-Anhänge mit potenziell gefährlichen Dateitypen (z.B. Dateitypen, die häufig von Viren verwendet werden) müssen automatisch gelöscht werden. Die Liste der blockierten

[1] Siehe Anhang B.1.4

[2] Siehe Anhang B.1.5

[3] Siehe Anhang B.1.6

[4] Siehe Anhang A.1.2

Dateitypen[5] wird von den zuständigen Stellen[6] verwaltet. Wenn eine E-Mail gelöscht wird, müssen gesellschaftsspezifische Regelungen[7] beachtet werden.

1.3.4 Filtern von unerwünschten E-Mails (SMTP)

Der gesamte E-Mail-Verkehr aus dem Internet muss von geeigneten Filterprodukten auf nicht angeforderte Massen-E-Mails (Unsolicited Bulk Emails, UBE) und nicht angeforderte kommerzielle E-Mails (Unsolicited Commercial Emails, UCE) gescannt werden. E-Mails, die einer dieser Kategorien angehören, müssen mit dem Zusatz [SPAM] in der Betreffzeile versehen oder zurückgewiesen werden.

Wenn eine E-Mail zurückgewiesen wird und nicht beim Empfänger ankommt, müssen gesellschaftsspezifische Regelungen[8] beachtet werden.

1.3.5 eMails versenden

Nicht authentisiertes Versenden von neuen Emails ist nicht zulässig. Mail Transfer Agents dürfen nicht als “open relay” konfiguriert werden.

[5] Siehe Anhang B.1.3

[6] Siehe Anhang B.1.7

[7] Siehe Anhang B.1.8

[8] Siehe Anhang B.1.9

2. Remote-Zugriff/VPN

2.1. Ziel

Das Ziel dieses Kapitels ist die Definition von Sicherheitsanforderungen für den Remote-Zugriff via VPN (Client-to-Site) zum Netzwerk des Audi Konzerns. Der Remote-Zugriff ermöglicht es Benutzern, sich über ein externes Netzwerk am internen Netzwerk von Audi anzumelden und die Ressourcen darin zu verwenden.

Dies umfasst beispielsweise:

- Verbindungen von tragbaren Computern (z. B. Laptops von Support-Mitarbeitern, die nicht vor Ort arbeiten oder unterwegs sind. Mobile Geräte, wie Tablets und Smartphones, gehören nicht zum Geltungsbereich)
- Management-Zugriffe auf interne Systeme (z. B. für Remote-Wartungen)
- Zugriff durch externe Mitarbeiter

2.2. Zugriff durch interne Mitarbeiter

2.2.1 Allgemeine Regelungen

- Nur die von der zuständigen Stelle[9] freigegebenen Remote-Zugriffsdienste dürfen verwendet werden.
- Die Infrastrukturabteilung[10] der entsprechenden Konzerngesellschaft ist für die Installation und den Betrieb der Infrastrukturkomponenten verantwortlich, die für den Zugriff auf das Netzwerk des Konzerns erforderlich sind (z. B. Router, Gateways).
- Die zuständigen Stellen müssen ein Betriebskonzept[11] für die Verwendung der Zugriffsinfrastruktur entwickeln, das die technischen Grundlagen für den Betrieb definiert. Das Konzept muss erforderliche Sicherheitsmaßnahmen umfassen.
- Die zuständigen Stellen[12] müssen (z. B. über ein Managementsystem) die Überwachung der Einhaltung der Anforderungen aus diesem Abschnitt implementieren.
- Jeder Benutzerzugriff muss durch die vom Konzern freigegebene starke Benutzerauthentifizierung[13] am Zugriffspunkt zum Netzwerk des Konzerns (Gateway) streng geprüft werden.
- Die Kommunikation zwischen Client und Gateway muss durch Verschlüsselung[14] gesichert werden. Die rechtlichen Bestimmungen des Landes, in dem das Endgerät verwendet wird, sind einzuhalten. Falls keine Verschlüsselung erlaubt ist, darf die Genehmigung zur Verwendung von Remote Access nicht erteilt werden.

[9] Siehe Anhang B.2.3

[10] Siehe Anhang B.2.5

[11] Siehe Anhang B.2.1

[12] Siehe Anhang B.2.2

[13] Siehe Anhang A.1.5

[14] Siehe Anhang A.1.9

- Es muss sichergestellt werden, dass der Client während der Verbindung mit dem Netzwerk des Audi-Konzerns keine weiteren Verbindungen herstellen kann. „Split-Tunneling“ ist nicht zulässig. Es ist nur eine einzelne Tunnelverbindung zum Netzwerk des Konzerns (VPN-Verschlüsselungsdomäne) erlaubt.
- Die Anforderungen der Regelungen für Clients[15] müssen beachtet werden.
- Remote-Zugriffsverbindungen vom Client zum Netzwerk des Audi Konzerns müssen nach einer Inaktivität von acht Stunden automatisch getrennt werden. Es ist untersagt, die Verbindung mithilfe von Netzwerkprozessen (z. B. Ping) aufrechtzuerhalten.
- Gerätezertifikate oder ähnliche Maßnahmen müssen implementiert werden, um den Client zu identifizieren.
- Wenn die Verwendung von VPN nicht mehr erforderlich ist, ist die zuständige Stelle[16] sofort zu informieren, damit sie die Blockierung des VPN-Zugriffs für bestimmte Client-Geräte und/oder Benutzer einleiten kann.
- Es muss sichergestellt werden, dass Verbindungsversuche, hergestellte Verbindungen und beendete Verbindungen am Zugriffspunkt zum Netzwerk des Konzerns (Gateway) protokolliert werden. Protokolldateien müssen mindestens folgende Informationen enthalten[17]:

- Datum/Uhrzeit,
- Quell-IP-Adresse,
- Ziel-IP-Adresse,
- Aufgelöste Hostnamen,
- Benutzer-ID,
- Erfolg/Fehler mit Grund.

- Verbindungsversuche müssen am Zugriffspunkt zum Netzwerk des Audi Konzerns abgewiesen werden und bestehende Verbindungen müssen sofort getrennt werden, wenn ein Verstoß gegen eine der obigen Anforderungen festgestellt wird. Clients können in einen Quarantänebereich zur Behebung verschoben werden, wenn auf keine anderen internen Ressourcen zugegriffen werden kann.

2.3. Spezielle Regelungen für den Zugriff durch externe Mitarbeiter

Zusätzlich zu den Anforderungen aus Kapitel 2.2.1 sind folgende Anforderungen zu beachten:

- Der Zugriff auf das Netzwerk des Konzerns muss für Mitarbeiter externer Unternehmen eingeschränkt sein (kein voller Zugriff). Es muss sichergestellt werden, dass Mitarbeiter externer Unternehmen nur Zugriff auf die Systeme im Netzwerk des Konzerns erhalten, die zur Erfüllung ihrer vertraglichen Verpflichtungen erforderlich sind. Die Netzwerkkommunikation muss auf die erforderlichen Protokolle/Ports und Zieladressen beschränkt sein.

[15] Siehe Anhang A.1.11

[16] Siehe Anhang B.2.4

[17] Siehe Anhang A.1.10

- Remote-Zugriffsdienste für externe Unternehmen müssen bei der Abteilung angefordert werden, für die das externe Unternehmen arbeitet. Diese Abteilung ist verantwortlich für jegliche Risiken, die sich daraus ergeben

3. Zugriff auf das Konzernnetzwerk

3.1. Ziel

Dieses Kapitel legt Sicherheitsanforderungen für den Zugriff über kabelbasiertes (LAN) fest. Die Anforderungen für Funknetzwerke (WLAN) sind in der entsprechenden Regelung[18] enthalten.

3.2. Prinzipien

Das primäre Ziel ist der Schutz des Konzernnetzwerks vor unbefugtem Zugriff. Dazu wird eine NAC-Lösung implementiert, mit der unbekannte Endgeräte blockiert werden können. Der Zugriff auf interne Ressourcen des Konzerns über LAN darf nur für authentifizierte und entsprechend autorisierte Geräte zugelassen werden.

Aus diesem Grund muss eine NAC-Lösung (Network Access Control) zur Authentifizierung von Geräten, die sich über ein Kabel mit dem Büronetzwerken verbinden, implementiert werden.

Für Produktionsumgebungen sollte eine NAC-Lösung[19] [20] implementiert werden.

3.3. Allgemeine Regelungen

3.3.1 Authentifizierung

- NAC muss im Zugriffsbereich des Netzwerks betrieben werden, d. h. auf der Ebene der Netzwerk-Ports, die für Endpunktverbindungen im LAN dediziert sind.
- Geräteauthentifizierung muss verwendet werden.
- Endgeräte sollten mit IEEE 802.1X authentifiziert werden. EAP-TLS sollte als bevorzugte EAP-Methode verwendet werden.
- Wenn ein System die automatisierte Zertifikatsverwaltung nicht ausreichend unterstützt, kann eine alternative Authentifizierungsmethode verwendet werden, falls diese von der zuständigen Stelle[21] für jeden Anwendungsfall und Gerätetyp freigegeben wurde.
- Neu erworbene Geräte müssen IEEE 802.1X und EAP-TLS mit Techniken für die automatisierte Zertifikatsverwaltung unterstützen.

3.3.2 Autorisierung

Die Autorisierung muss auf Grundlage des Authentifizierungsergebnisses vorgenommen werden, indem das Endgerät einer Netzwerkzugriffsregel zugewiesen wird:

- Endgeräte, die sich mit IEEE 802.1X und EAP-TLS (oder einer vergleichbaren EAP-Methode) authentifizieren, müssen der vertrauenswürdigen Zugriffsregel zugewiesen werden, die uneingeschränkte Kommunikation für die Gerätegruppe erlaubt.

[18] Siehe A.1.8

[19] Siehe Anhang A.1.13

[20] Siehe Anhang A.1.6

[21] Siehe Anhang B.3.1

- Endgeräte, die sich nicht mit IEEE 802.1X und EAP-TLS (oder einer vergleichbaren EAP-Methode) authentifizieren, jedoch beispielsweise anhand ihrer MAC-Adresse authentifiziert werden, müssen einer eingeschränkten Zugriffsregel zugewiesen werden, die nur beschränkte Kommunikation zulässt.

- Endgeräte, die sich nicht oder nicht erfolgreich authentifizieren, müssen einer nicht vertrauenswürdigen Zugriffsregel zugewiesen werden. Die nicht vertrauenswürdige Zugriffsregel darf nur eine sehr eingeschränkte Kommunikation bereitstellen und nur einfache für die Fehlerbehebung des Geräts erforderliche Protokolle zulassen. Der Zugriff auf andere interne Ressourcen muss verhindert werden.

3.4. Spezielle Regelungen

- Methoden zum expliziten Verweigern des Zugriffs von Geräten auf das Netzwerk müssen implementiert werden.
  - Für Geräte, die IEEE 802.1X und EAP-TLS unterstützen, muss eine Zertifikatsperrliste (CRL) verwaltet werden. Diese CRL muss überprüft werden, bevor Zugriff auf das Netzwerk gewährt wird.
  - Für Geräte, die über MAC-Adressen authentifiziert werden, muss die Adresse überprüft werden, bevor Zugriff auf das Netzwerk gewährt wird.
- Notfallverfahren zum Deaktivieren der Netzwerkzugriffskontrolle (NAC) müssen bereitgestellt werden.
  - Das Deaktivieren der Netzwerkzugriffskontrolle bei einem Notfall/Fehler muss festgelegten Verfahren folgen und zulässige Aktionen definieren (Deaktivieren der NAC-Funktion eines einzelnen Switches, im gesamten Netzwerk usw.).
- Verfahren zum Gewähren von temporärem Netzwerkzugriff für nicht authentifizierte Geräte sollten implementiert werden.
- Temporärer Zugriff kann folgendermaßen gewährt werden:
  - Vom Servicedesk nach der Überprüfung des Benutzers
  - Durch die Authentifizierung des Benutzers (z. B. Webportal)

4. Anbindung neuer Gesellschaften

4.1. Ziel

Ziel dieses Kapitels ist die Festlegung von Voraussetzungen und die Beschreibung der Verfahren zur Anbindung neuer Gesellschaften an das Netzwerk des Konzerns.

4.2. Prinzipien

4.2.1 Allgemeine Regelungen

- Nur Gesellschaften, die im Mehrheitsbesitz[22] des Konzerns sind, dürfen Zugriff auf das Netzwerk des Konzerns erhalten.
- Es muss gewährleistet werden, dass der rechtliche Rahmen des Landes, in dem die Gesellschaft (oder die Tochtergesellschaft) ihren Sitz hat, die IT-Infrastruktur des Konzerns nicht beeinträchtigt (z. B. durch das Verbot von Schutzmaßnahmen wie Verschlüsselung).
- Die Gesellschaft muss die Einhaltung der vom Konzern bereitgestellten Informationssicherheitsregelungen gewährleisten (die Regelungen sind zugänglich zu machen). Dies muss schriftlich vom Management[23] bestätigt werden.
- Falls Gesellschaften die Informationssicherheitsregelungen nicht (oder nicht dauerhaft) einhalten, darf ihre Anbindung zum Netzwerk des Konzerns jederzeit getrennt werden.

4.2.2 Verfahren

- Um die Anbindung anzufordern, muss sich die Gesellschaft an die zuständige Stelle[24] wenden. Die Gesellschaft muss ein Self-Assessment (VDA/ISA[25]) bereitstellen.
- Die zuständige Stelle verwaltet alle Anträge, Informationen, Genehmigungen und Ablehnungen von Verbindungen und Trennungen zentral.

[22] Mehr als 50%

[23] Durch das verantwortliche Management und den CISO

[24] Siehe Anhang B.4.4

[25] Siehe Anhang A.2.1

5. Anbindung externer Büroumgebungen

5.1. Ziel

Dieses Kapitel legt die Grundvoraussetzungen für die Anbindung von externen Büroumgebungen außerhalb Gesellschaftsgrenzen / Werksgrenzen fest, die mit dem Konzernnetzwerk verbunden sind. Die entsprechenden Büroumgebungen können sich dabei in gesellschaftseigenen oder angemieteten Gebäuden befinden. Darüber hinaus kann es sich um einzelne von Audi angemietete Büroräume in einem Gebäudekomplex eines Dritten handeln.

5.2. Prinzipien

Die Erweiterung des Konzernnetzwerks auf physische Bereiche außerhalb der Gesellschaft stellt ein potenzielles Risiko dar, da dies den direkten Zugriff auf Ressourcen im Netzwerk ermöglicht. Dieser Zugriff erfordert besondere Kontrolle. Vor der Erweiterung des Netzwerks des Konzerns muss die Verwendung anderer Lösungen (z. B. Internet, VPN für Interne) auf ihre Eignung hin überprüft werden.

Um das Risiko des Missbrauchs von Ressourcen zu minimieren, müssen Anbindungen an das Konzernnetzwerk die folgenden Anforderungen erfüllen:

- Eine Audi Konzerngesellschaft muss die Schlüsselgewalt besitzen. Der Zutritt muss von der Konzerngesellschaft kontrolliert werden. Um dies zu gewährleisten, muss ein elektronisches Zutrittssystem eingerichtet werden oder die Schlüsselgewalt für die entsprechenden Räumlichkeiten muss bei der Konzerngesellschaft liegen.
- Nur genehmigte Netzwerkverbindungen für das Netzwerk des Konzerns dürfen verwendet werden. Diese müssen von der zuständigen Stelle[26] freigegeben werden. Diese Stelle muss einen zentralen Überblick über die angebundenen externen Büroumgebungen haben.
- Die Konzerngesellschaft, die die Umgebung anbindet, ist verantwortlich für die installierte Netzwerkinfrastruktur.
- Die Audi Konzerngesellschaft muss die Netzwerkinfrastruktur auf Verbindungen zu Netzen Dritter überprüfen und diese Verbindungen auf angemessene Sicherheitsmaßnahmen hin untersuchen.
- Die Clients (PCs/Workstations) und alle Serversysteme werden von einer Konzerngesellschaft bereitgestellt und sind hinsichtlich Softwareupdates und Maßnahmen zum Schutz vor Viren in die Prozesse der Konzerngesellschaft integriert.
- Auszüge aus Büroumgebungen, für die eine Anbindung zum Netzwerk des Konzerns besteht, müssen der zuständigen Stelle[27] rechtzeitig gemeldet werden. Der nächste Mieter darf keinen Zugriff auf das Netzwerk des Audi-Konzerns erhalten.

[26] Siehe Anhang B.5.1

[27] Siehe Anhang B.5.2 und B.5.3

6. Anbindung von Partnerunternehmen, Importeuren und Händlern

6.1. Ziel

Ziel dieses Kapitels ist die Definition von Voraussetzungen und Verfahren zur Anbindung externer Partner, Importeure oder Händler mit den dedizierten Netzwerkumgebungen (Extranets) des Konzerns. Dies schließt die Anbindung über Remote-Access Lösungen mit ein.

Dieses Kapitel umfasst nur Anforderungen für Netzwerkzugänge. Weitere, ggf. zu beachtende Regelungen, sind nicht enthalten.

6.2. Prinzipien

Ein externer Partner, Importeur oder Händler, ist eine Gesellschaft, die einmalig, gelegentlich oder auf regelmäßiger Basis mit dem Konzern zusammenarbeitet und eine vertragliche Beziehung zu einer Konzerngesellschaft hat, die nicht im Mehrheitsbesitz des Konzerns ist. Diese können Zugriff auf Systeme und Daten des Konzerns erhalten, die sie zur Erfüllung ihrer Aufgaben benötigen.

6.3. Grundlegende Anforderungen

Die technische Lösung der Netzwerkanbindung (z.B. dedizierte Netzwerkumgebungen wie PFN – Partner Firmen Netzwerk, CPN – Central Partner Network oder Remote-Access Lösungen) müssen von der zuständigen Stelle freigegeben sein. Anforderungen sind:

- Es besteht ein gültiger Vertrag zwischen Partner und Konzern
- Es besteht eine gültige Geheimhaltungsvereinbarung (NDA) zwischen Partner und Konzern
- Die Anforderungen des VDA/ISA sind erfüllt[28].

6.4. Verfahren

- Der externe Partner/Importeur/Händler wendet sich an den verantwortlichen Geschäftsbereich, welcher Vertragseigener ist, um die Anbindung an ein Extranet anzufordern. Die folgenden Informationen sind bereitzustellen:
    - Liste mit Anwendungen, auf die externe Partner/Importeure/Händler zugreifen möchten
    - Dokumentation über den Vertrag, speziell die erwartete Laufzeit
    - Geheimhaltungsvereinbarung (NDA)
    - Schriftliche Bestätigung der Erfüllung der Anforderungen des VDA/ISA[29]
- Die zuständige Stelle muss umgehend informiert werden, wenn die Anbindung eines Partnerunternehmens getrennt wird.

[28] Siehe Anhang A.2.1

[29] Siehe Anhang A.2.1

- Die zuständige Stelle verwaltet zentral alle Anträge, Informationen, Genehmigungen und Ablehnungen von Anbindungen und Trennungen.

6.5. Einrichtung des Zugriffs

Die Einrichtung des Zugriffs auf Systeme im Extranet muss dem Schema zur Datenklassifizierung/-authentifizierung entsprechen[30]. Die für die Daten zuständige Abteilung gewährt eine fachliche Freigabe für die Anträge unter Berücksichtigung der Datenklassifizierung. Die IT-Sicherheitsgenehmigung wird durch die zuständige Stelle erteilt.

Zugriff auf Anwendungen im Netzwerk des Audi-Konzerns wird nur gewährt, wenn eine starke Authentifizierung an einer zentralen Stelle im Extranet durchgeführt wurde. Gleichzeitig muss sichergestellt werden, dass Verbindungen und Verbindungsversuche protokolliert werden. Eine direkte Verbindung eines externen Partners/Importeurs/Händlers zum Netzwerk des Audi-Konzerns ist nicht erlaubt.

Direkte Server-zu-Server-Kommunikation zwischen dem Extranet und dem Konzernnetzwerk (z. B. Anwendung im Extranet und Datenbank im Netzwerk des Konzerns) ist zulässig, muss jedoch protokolliert werden. Aus Sicherheitsgründen sollte ein Proxy eingesetzt werden.

[30] Siehe Anhang A.1.5

II. Verantwortlichkeiten

II.I Kapitel 1: Content Filtering

Diese Regelung ist von allen Betreibern von Content Filtering anzuwenden und einzuhalten.

Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur in Abstimmung mit der IT-Sicherheit und grundsätzlich nur zeitlich begrenzt zulässig.

II.II Kapitel 2: Remote-Zugriff

Diese Regelung ist von allen Betreibern von Remote-Zugriffsdiensten für das Netzwerk des Audi-Konzerns anzuwenden und einzuhalten.

Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur in Abstimmung mit der IT-Sicherheit und grundsätzlich nur zeitlich begrenzt zulässig.

II.III Kapitel 3: Zugriff auf das Konzernnetzwerk

Diese Regelung ist von allen Betreibern von Zugriffen auf das Konzernnetzwerk anzuwenden und einzuhalten.

Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur in Abstimmung mit der IT-Sicherheit und grundsätzlich nur zeitlich begrenzt zulässig.

II.IV Kapitel 4: Anbindung neuer Gesellschaften

Diese Regelung muss von allen Stellen angewendet und eingehalten werden, die Anbindungen zum Netzwerk des Konzerns genehmigen und betreiben.

Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur in Abstimmung mit der IT-Sicherheit und grundsätzlich nur zeitlich begrenzt zulässig.

II.V Kapitel 5: Anbindung externer Büroumgebungen

Diese Regelung muss von allen Stellen angewendet und eingehalten werden, die Anbindungen zum Netzwerk des Konzerns implementieren und betreiben. Die zuständigen Manager tragen unternehmerische Verantwortung für die entsprechenden Büroumgebungen.

Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur in Abstimmung mit der IT-Sicherheit und grundsätzlich nur zeitlich begrenzt zulässig.

II.VI Kapitel 6: Anbindung von Partnerunternehmen, Importeuren und Händlern

Diese Regelung muss von allen Organisationseinheiten angewendet und eingehalten werden, die Anbindungen von Partnerunternehmen zum Netzwerk des Konzerns genehmigen und betreiben.

Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur in Abstimmung mit der IT-Sicherheit und grundsätzlich nur zeitlich begrenzt zulässig.

Anhang

A. Allgemeines

A.1 Mitgeltende Dokumente

A.1.1 Informationssicherheit Regelung Nr. 03.01.09 Ausnahmeprozess

A.1.2 Informationssicherheit Regelung Nr. 03.01.01 Anti Malware & Systemschutz

A.1.3 Informationssicherheitshandlungsleitlinien für Mitarbeiterinnen und Mitarbeiter

A.1.4 Informationssicherheitshandlungsleitlinien für Partnerfirmen

A.1.5 Informationssicherheit Regelung Nr. 03.01.05 Authentifizierung und IAM

A.1.6 Informationssicherheit Regelung Nr. 03.01.19 Virtualisierung (Kapitel 3.10)

A.1.7 ITSP P11.2 Secure Environment Concept

Für eine generelle Beschreibung: https://group-wiki.wob.vw.vwg/wikis/pages/viewpage.action?pageId=124158158

A.1.8 Informationssicherheit Regelung Nr. 03.02.01 Funknetzwerke

A.1.9 Informationssicherheit Regelung Nr. 03.01.02 Kryptographie

A.1.10 Informationssicherheit Regelung Nr. 03.01.04 Sicherheitsprotokollierung und -monitoring

A.1.11 Informationssicherheit Regelung Nr. 03.03.02 Clients

A.1.12 Informationssicherheit Regelung Nr. 03.01.01 Anti Malware & Systemschutz

A.1.13 Informationssicherheit Regelung Nr. 03.01.20 Informationssicherheit in Produktionsumgebungen

A.2 Anlagen

A.2.1 Anlage 1 Feedbackformular

Das Feedbackformular für Änderungsvorschläge zu Regelungen kann von der MyNet-Webseite Gesellschaften → Audi Brussels → Organisation → Finanz (B/F) → IT (B/FP) → IT-Sicherheit → Regelwerk heruntergeladen werden.

Das Feedback-Formular ist folgendermaßen auszufüllen:

Die Spalten 2 bis 6 müssen für jede vorgeschlagene Änderung ausgefüllt werden. Änderungen, für die nicht alle Spalten 2 bis 6 ausgefüllt sind, werden automatisch ohne weitere Prüfung abgelehnt.

Spalte 3: Folgende Kommentararten sind möglich: a=allgemein, f=fachlich, r=redaktionell

Spalte 4: Bitte bisherigen Text, Tabelle oder Bild einfügen

Spalte 5: Bitte vollständig umformulierten Text, geänderte Tabelle oder geändertes Bild einfügen

Spalte 6: Bitte begründen Sie die gewünschte Änderung möglichst ausführlich.

Bitte senden Sie das ausgefüllte Formular an: it-security.audibx@audi.de

A.2.2 Dies erfolgt durch ein TISAX Testat der entsprechenden Gesellschaft/Partnerunternehmen

A.3 Abkürzungen und Definitionen

Begriff	Definition
CPN	Central Partner Network
PFN	Partner Firmen Netzwerk
Group Network	Public, Restricted, Production, Administration, Classified Clients, Infrastructructure Services

A.4 Gültigkeit

Diese Regelung ist mit der Veröffentlichung sofort gültig.

Bereits bestehende Ausnahmeregelungen sind spätestens bei der nächsten Änderung (z.B. Verlängerung, Änderung der Auflagen) an diese Regelung anzupassen.

Nächster Überprüfungstermin: 06.08.2021

Für die Meldung von Änderungswünschen verwenden Sie bitte das vorgegebene Formular[31].

A.5 Dokumentenhistorie

Version	Name	Org.-Einheit	Datum	Bemerkung
1.0	Andreas Walter	B/FP	07.08.2019	Veröffentlicht

[31] Siehe Anhang A.2.1 Anlage 1 Feedbackformular

B. Spezifische Ausprägungen

B.1 Kapitel 1: Content Filtering

B.1.1 Protokolle und Ports

Dienst / Protokoll	Port	Beschreibung
FTP	20 und 21	Nur nach Freigabe der IT-Sicherheit
SFTP	22	Nur nach Freigabe der IT-Sicherheit
HTTP	80	Surfen im Internet (unverschlüsselt)
HTTPS	443	Surfen im Internet (verschlüsselt)
SMTP	25	Ausgehende E-Mails: Diese Verbindung ist nur für zentrale E-Mail-Server erlaubt.

Änderungen sind nur in Zusammenarbeit mit der IT-Sicherheit möglich.

B.1.2 IT-Sicherheit

B.1.3

Dateityp	*Beschreibung*
.bas	*Microsoft Visual Basic Class Module*
.bat	*Batch File*
.chm	*Compiled HTML Help File*
.cmd	*Microsoft Windows NT Command Script*
.com	*MS-DOS Application*
.cpl	*Control Panel Extension*
.exe	*Program*
.hlp	*Help File*
.hta	*HTML Program*
.inf	*Installation Script*
*.js**	*Javascript File*
.lnk	*Link Shortcut*
.pif	*Program Information File, Shortcut to MS-DOS Program*
.reg	*Registration Entries*

.scr	*Screen Saver*
.shs	*Shell Scrap Object*
*.vb**	*VB Script Files*
*.ws**	*Windows Script Files*
.ps1	*Powershell Script Files]*

B.1.4 Keine weiteren Details

B.1.5 Keine weiteren Details

B.1.6 Keine weiteren Details

B.1.7 IT-Sicherheit

B.1.8 Keine weiteren Details

B.1.9 Keine weiteren Details

B.2 Kapitel 2: Remote Zugriff

B.2.1 Auf Grundlage von Anforderungen die durch die IT-Sicherheit definiert wurden.

B.2.2 IT-Services

B.2.3 IT-Sicherheit

B.2.4 IT-Services

B.2.5 IT-Services

B.2.6 IT-Sicherheit

B.3 Kapitel 3: Zugriff auf das Konzernnetzwerk

B.3.1 IT-Sicherheit

B.4 Kapitel 4: Anbindung neuer Gesellschaften

B.4.1 IT-Sicherheit

B.4.2 IT-Services

B.4.3 Verpflichtungserklärung zur Einhaltung des Informationssicherheitsregelwerkes (kann bei der IT-Sicherheit angefragt werden)

B.4.4 IT Integration Gesellschaften

B.5 Kapitel 5: Anbindung externer Büroumgebungen

B.5.1 IT-Services

B.5.2 IT-Services

(Die grundsätzlichen Netzwerkanbindungsarten, die bei Audi zum Einsatz kommen dürfen, müssen von der IT-Sicherheit im Vorfeld freigegeben werden.)

B.5.3 Der jeweilige Hausherr

B.6 Kapitel 6: Anbindung von Partnerunternehmen, Importeuren und Händlern

B.6.1 -