Besondere Anforderungen Informationssicherheit

Verwendung für Anforderungen der e-netz Südhessen GmbH & Co.KG s in Verbindung mit

informationssicherheitsrelevanten Lieferanten und Dienstleistern der Kategorien Typ 1, Typ 2 und Typ 3

Besondere Anforderungen Informationssicherheit

Inhaltsverzeichnis:

Besondere Anforderungen Informationssicherheit

Zweck

IKT-Systeme, ICS und angebotene IKT-Dienstleistungen im Geltungsbereich des ISMS müssen nach anerkanntem Stand der Technik in der Informationssicherheit gemäß der Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) entwickelt, in Betrieb genommen, dokumentiert und betrieben werden. Details der vorgesehenen Sicherheitsmaßnahmen sind im Angebot sowohl in technischen als auch organisatorischen Belangen zu beschreiben. Die Anforderungen nach § 11 EnWG sowie insbesondere der IT-Sicherheitskatalog der BNetzA sind einzuhalten
Die Umsetzung der Anforderungen ist zu beschreiben. Alle Abweichungen davon sind im Angebot zu benennen und zu begründen. Der Einsatz von Nachunternehmern und/oder Dritten ist nur mit vorheriger schriftlicher Zustimmung des Auftraggebers zulässig. Der Auftragnehmer hat für alle Nachunternehmer wie für sein eigenes Handeln einzustehen.

Geltungsbereich und Zielgruppen

Dieser Vertragsbestandteil enthält die Anforderungen an Drittunternehmen, um die Sicherheitsanforderungen der e-netz Südhessen GmbH & Co. KG zu gewährleisten.

Die nachfolgenden Anforderungen sind verbindlicher Bestandteil der Liefer- und Wartungsverträge. Jegliche Abweichungen von den Anforderungen sind dem Auftraggeber (im Folgenden AG genannt) schriftlich mitzuteilen und von diesem explizit zu genehmigen.

Drittunternehmen (im Folgenden Dienstleister oder DL genannt), die Dienstleistungen oder Produkte im Geltungsbereich des ISMS erbringen oder liefern, müssen grundlegende Anforderungen an die Sicherheit ihrer informationsverarbeitenden Systeme erfüllen und geeignete organisatorische Abläufe in Bezug auf sichere interne IT-Abläufe zusichern. Der AG behält sich vor, für unten genannte Maßnahmen entsprechende Nachweise anzufordern.

Werden Subdienstleister durch den DL eingesetzt, so sind diese Anforderungen ebenfalls für den Subdienstleister bindend. Der Einsatz von Subdienstleistern ist dem AG anzuzeigen.

1 Informationssicherheitsprozess

1.1 Geregelter Sicherheitsprozess zur Steuerung und Verbesserung der Informationssicherheit (T1, T2, T3)

Der Dienstleister muss in seinem Unternehmen einen geeigneten Sicherheitsprozess zur Planung, Steuerung, Kontrolle und Verbesserung der Informationssicherheit etabliert haben, über den die Umsetzung der hier geforderten technischen und organisatorischen Maßnahmen sichergestellt wird.

Dies kann beispielsweise in Form eines Informations-Sicherheitsmanagementsystems (ISMS) bzw. einer Zertifizierung nach ISO/IEC 27001 oder der Steuerung interner Abläufe bzw. des Betriebs der IT-Infrastruktur, z. B. nach ITIL, erfolgen. Der Nachweis einer Zertifizierung und/oder eines Lieferantenaudits kann in begründeten Einzelfällen erforderlich werden.

Der Dienstleister hat bei Einsatz von Subdienstleistern und Drittherstellter-Produkten diese zu benennen sowie die Umsetzung der Anforderungen aus der Dienstleistungsvereinbarung sicherzustellen und zu dokumentieren.

1.2 Ansprechpartner für Informationssicherheit (T1, T2, T3)

Der Dienstleister verfügt über einen Ansprechpartner zur Informationssicherheit, der für die Umsetzung und Überprüfung von Informationssicherheitsmaßnahmen verantwortlich und der zu Fragen der Informationssicherheit gegenüber dem Auftraggeber auskunftsfähig und auskunftsberechtigt ist.

Die vollständigen Kontaktdaten des Ansprechpartners sind dem AG mitzuteilen.

1.3 Mitarbeiter und Dienstleister (T2, T3)

Die Mitarbeiter und Subdienstleister des DL sind über die sicherheitstechnischen Anforderungen des AG zu informieren.

Die besondere Bedeutung der Informationssicherheit muss durch entsprechende Security-Schulungen für Mitarbeiter des DL unterstrichen werden. Dabei sind die besondere Sensibilität im Umgang mit vertraulichen und sensiblen Daten sowie die sicherheitstechnischen Anforderungen herauszustellen.

Die Mitarbeiter müssen hinsichtlich des vertraulichen Umgangs mit Informationen, die ihnen im Zuge ihrer Tätigkeit bekannt werden, verpflichtet werden. Dies kann bspw. durch entsprechende Regelungen im Arbeitsvertrag oder eine separate Erklärung erfolgen.

Scheiden Mitarbeiter des DL aus dem Unternehmen aus oder wechseln ihr Aufgabengebiet, ist durch geeignete Maßnahmen sicherzustellen, dass sicherheitssensitive Zutritts- und Zugriffsberechtigungen zu Systemen und Informationen des AG entzogen werden sowie Einwahlmöglichkeiten dieser Mitarbeiter in das Daten- / Prozessnetz und die Fernwartungsumgebung des AG ausgeschlossen sind. Die Accounts der betroffenen Mitarbeiter sind zumindest zu deaktivieren.

Der AG behält sich vor, für oben genannte Maßnahmen entsprechende Nachweise anzufordern.

Der AG behält sich vor, Mitarbeiter von Dienstleistern, die in Kontakt mit als besonders sensibel kategorisierten Informationen oder Anlagen kommen, einer Sicherheitsüberprüfung unterziehen zu lassen bzw. für diese einen entsprechenden Sicherheitsnachweis einzufordern.

Werden Subdienstleister durch den DL eingesetzt, so sind diese Anforderungen ebenfalls für den Subdienstleister bindend. Der Einsatz von Subdienstleistern ist dem AG anzuzeigen.

1.4 Anforderungen zum Stand der Technik (T2, T3)

Der DL hat die Verfahren zur Etablierung des Stands der Technik darzustellen, dazu gehört zum Beispiel die Beschreibung der Anforderungserfüllung gemäß des BDEW Whitepaper "Anforderungen an sichere Steuerungs- und Telekommunikationssysteme". Zu diesem Zweck stellt der AG auf Anfrage dieses Whitepaper sowie eine Übersicht der relevanten Standards und Anforderungen zur Leistungserbringung zur Verfügung.

Der Nachweis der Anforderungserfüllung kann durch vorhandene Zertifierungen erbracht werden (z.B. Produktzertifizierung nach IEC 62443).

(T3) In Abstimmung mit dem AG erfolgt die Dokumentation der Informationssicherheitsanforderungen in Form eines Pflichtenheftes durch den DL.

2 Technische und organisatorische Bestimmungen

2.1 Zugriffs- und Zutrittsschutz (T1, T2, T3)

(T1, T2) Räume oder Bereiche beim Dienstleister, in denen Informationen elektronisch verarbeitet oder gespeichert werden, müssen durch geeignete Maßnahmen vor unberechtigtem Zutritt geschützt werden.

(T3) Alle informationsverarbeitenden Systeme des DL, von denen ein Zugriff auf die Systemumgebung des AG oder dem AG zugeordnete sensible Informationen mittelbar oder unmittelbar möglich ist, müssen mit einem sicheren logischen Zugangsschutz versehen sein. Dabei ist eine Multi-Faktor-Authentifizierung anzustreben (z. B. Kombination aus Benutzername/Passwort und einer ergänzenden Identifizierung mit Hilfe eines Hardwaretokens, einer Smartcard o. Ä. oder eines biometrischen Merkmals).

2.2 Kennwortanforderungen (T3)

An die Kennwörter für informationsverarbeitende Systeme und Komponenten werden besondere Anforderungen gestellt, der DL muss deshalb eine verpflichtende Kennwortrichtlinie definiert haben.

Diese Richtlinie muss mindestens den Anforderungen an Kennwörter des AG entsprechen. Diese Anforderungen wird der AG dem DL zur Verfügung stellen.

2.3 Netzwerksicherheit (T2, T3)

Das interne Datennetzwerk des DL wird von öffentlichen oder externen Netzen durch geeignete Maßnahmen nach dem Stand der Technik getrennt (z. B. Firewall).

Drahtlose Netzwerke müssen nach Stand der Technik gesichert werden, insbesondere muss ein unbefugter Zugriff auf die System- und Wartungsumgebung des AG oder dem AG zugeordnete sensible Informationen sicher verhindert werden.

2.4 Schadsoftwareschutz (T3)

Der DL muss sicherstellen, dass alle informationsverarbeitenden Systeme mit einem aktiven und aktuellen Schutz vor Schadsoftware versehen sind, soweit sich dies technisch realisieren lässt.

Insbesondere für diejenigen Systeme, von denen mittel- oder unmittelbar Zugriffe auf die System- und Wartungsumgebung des AG möglich sind (z. B. Parametrierlaptops, Terminalserver, Web-, Mail- und Dateiserver usw.) ist ein stringenter Schadsoftwareschutz sicherzustellen.

Der DL muss sicherstellen, dass der Schadsoftwareschutz nicht durch Mitarbeiter deaktiviert wird.

Bei Pattern-basierten Lösungen ist dafür Sorge zu tragen, dass die Schadsoftware-Pattern unverzüglich aktualisiert werden.

Neben den Arbeitsplatzsystemen muss der Schutz vor Schadsoftware auch Kommunikationsverbindungen, wie Web-, E-Mail- und Datentransfer, umfassen.

2.5 Systemhärtung, Schwachstellen und Patch-Management (T3)

Systeme sind nach anerkannten und dokumentierten Verfahren (z. B. CIS-Standards) zu konfigurieren bzw. zu parametrieren, dazu gehört z. B. die dokumentierte Systemhärtung.

Betriebssysteme, Firmware oder Applikationen von IT-Komponenten des DL sind unverzüglich durch Softwareupdates des jeweiligen Herstellers zu aktualisieren, wenn durch diese Updates Sicherheitslücken geschlossen oder Schwachstellen beseitigt werden.

Zu diesem Zweck ist ein Patchmanagement zu etablieren, welches sicherstellt, dass Patches vom Hersteller bezogen sowie nach Dringlichkeit kategorisiert und durch einen geregelten Prozess installiert werden können.

3 Umgang mit klassifizierten Informationen (T1, T2, T3)

Der DL muss die Vorgaben zur Klassifizierung von Informationen des AG einhalten.

Alle Informationen des AG sind ihrer Vertraulichkeitsklasse entsprechend eindeutig eingeordnet und gekennzeichnet. Die Informationsklassifizierung richtet sich dabei nach dem möglichen Einfluss auf das Geschäft des AG, der sich aus einer vorsätzlichen oder nicht beabsichtigten Bekanntgabe der Informationen ergeben kann.

Der AG hat die nachfolgenden Vertraulichkeitsklassen festgelegt, aus denen sich jeweils unterschiedliche Konsequenzen für die Handhabung der relevanten Informationen ergeben.

Tabelle 1: Vertraulichkeitsklassen

Vertraulichkeits-klasse	Handhabung
(S0) - öffentlich	Daten, die entsprechend ihres Informationsgehaltes gezielt für eine allgemeine Publikation erstellt und entsprechend durch die Verantwortlichen des Unternehmens freigegeben wurden. Als Beispiel sind darunter Marketingunterlagen, Veröffentlichungen jedweder Art, Endkundenpreislisten usw. zu verstehen. Die Dokumente sind standardmäßig mit dem Vermerk "S0" und/oder "öffentlich" gekennzeichnet.
(S1) - Konzern-intern	Daten, die aufgrund ihres Inhalts entsprechend für Mitarbeiter und auf die Vertraulichkeit verpflichtete DL des gesamten Konzerns gedacht sind, jedoch Informationen enthalten, die nicht zur allgemeinen Veröffentlichung freigegeben wurden. Die Dokumente sind standardmäßig mit dem Vermerk "S1" und/oder "Konzern-intern" gekennzeichnet.
(S2) - intern	Daten, die aufgrund ihres Inhalts ausschließlich für Mitarbeiter und und auf die Vertraulichkeit verpflichtete DL einer Gesellschaft / eines Bereiches gedacht sind und Informationen enthalten, die nicht zur Veröffentlichung im gesamten Konzern freigegeben wurden. Dies gilt auch für Daten, deren Charakter einem Kommunikationsverhältnis zuzuordnen ist, welches einem individuellen Angebot gleich kommt. Als Beispiel sind Rechnungen, Angebote, Verträge mit Lieferanten, Kunden, oder Dienstleistern zu nennen. Die Dokumente sollten zur besseren Darstellung mit dem Vermerk "S2" und/oder "intern" gekennzeichnet werden.
(S3) - vertraulich	Daten, die aufgrund ihres Informationsgehaltes ausschließlich für den "internen Dienstgebrauch" erhoben bzw. erzeugt wurden sowie Daten, die gesetzlichen Regelungen (z. B. Bundesdatenschutzgesetz) unterliegen und eine Veröffentlichung über den Mitarbeiterkreis des Unternehmens, die diese Daten zur Erfüllung ihrer Aufgabe benötigen, hinaus untersagt sind. Als Beispiel sind Kalkulationen, personenbezogene Daten (Kunden und Mitarbeiter), interne Firmendaten (Kalkulationen, etc.) zu nennen. Die Dokumente sind standardmäßig mit dem Vermerk "S3" und/oder "vertraulich" gekennzeichnet.

Vertraulichkeits-klasse	Handhabung
(S4) - streng vertraulich	Daten, die aufgrund ihres Informationsgehaltes ausschließlich der Führungsebene und ihrem Aufgabengebiet zuzuordnen sind, sowie Daten die gesetzlichen Regelungen unterliegen und im juristischen Sinne als "Insiderwissen" klassifiziert werden. Dies können Vorstands- und Aufsichtsratsprotokolle sein, aber auch Infrastrukturzeichnungen, Strategiepapiere etc. Die Dokumente sind standardmäßig mit dem Vermerk "S4" und/oder "streng vertraulich" gekennzeichnet.

3.1 Verarbeitung sensibler Informationen (T1, T2, T3)

Zu den besonders schützenswerten Daten der Vertraulichkeitsklassen S3 und S4 des AG werden insbesondere die folgenden Informationen gezählt:

- Informationen zur Konfiguration und Implementierung von Sicherheitsmaßnahmen
- Passwörter und Authentisierungsinformationen
- Netzwerkpläne, -konfigurationen und IP-Adress-Informationen
- Aufbau und Konfiguration von Systemen und Komponenten der IT- und Prozessleittechnik des AG.

Diese Daten werden im Sinne der hier dargestellten Sicherheitsanforderungen auch als "sensibel" bezeichnet und können zusätzlich den oben aufgeführten Vertraulichkeitsstufen S3 und S4 unterliegen.

3.2 Zugriffsschutz, Speicherung und Entsorgung (T1, T2, T3)

Werden Daten des AG durch den DL verarbeitet, so hat dieser sicherzustellen, dass der Zugriff auf diese Daten auf einen minimalen Kreis berechtigter Mitarbeiter eingeschränkt wird.

Werden sensible Daten auf mobilen Komponenten gespeichert (z. B. Notebooks, mobile Datenträger etc.), sind diese durch eine Verschlüsselung nach Stand der Technik zu sichern.

Werden IT-Systeme oder Komponenten des DL, auf denen sensible Daten des AG gespeichert sind, zur Reparatur gegeben oder einer Entsorgung zugeführt, muss gewährleistet sein, dass diese Daten nicht für Dritte, auch nicht unter Verwendung von Daten-Wiederherstellungstechnologien, lesbar oder anderweitig auswertbar sind.

Der Stand der Technik zur sicheren Vernichtung von Informationen ist anzuwenden.

3.3 Übermittlung in Netzwerken (T1, T2, T3)

Datenverkehr, über den sensible Informationen zwischen AG und DL über ein unsicheres Netz (z. B. Internet) ausgetauscht werden, muss mit Hilfe anerkannter technischer Verfahren gegen Manipulation oder Einsichtnahme geschützt werden.

(T2, T3) Dafür sind in der Regel VPN-Lösungen einzusetzen, deren kryptographische Algorithmen dem aktuellen Stand der Technik entsprechen.

(T2, T3) Der VPN-Tunnel muss nach Beendigung der Kommunikation abgebaut werden; eine dauerhafte Einrichtung eines solchen Tunnels zwischen AG und DL ist untersagt.

(T1, T2, T3) Werden per E-Mail sensible Informationen zwischen AG und DL ausgetauscht, so muss der Mailverkehr kryptographisch gesichert werden. Der DL trägt Sorge für die entsprechenden technischen Voraussetzungen auf seiner Seite.

4 Anforderungen an die Wartungsprozesse (T2, T3)

Unter "Wartung" werden alle vom DL erbrachten Servicemaßnahmen verstanden, die sich auf die Komponenten oder Systeme der technischen IT-Umgebung des AG auswirken.

Servicemaßnahmen können beispielsweise sein:

- Instandhaltungs- und Reparaturarbeiten
- Fehleranalyse- und Fehlerbehebungsarbeiten
- Installation von Softwareupdates oder neuen Firmware- oder Betriebssystemen bzw. Applikationen
- System-, Geräte oder Software-Anpassungen, Neuparametrierungen u. Ä.

Wartungsarbeiten können innerhalb eines Remote-Zugriffs über eine Fernwartungsinfrastruktur bei DL und AG, als auch in Form von Vor-Ort-Arbeiten (z. B. Anschluss mobiler Geräte an das Netzwerk oder die IT- und Prozesstechnikkomponenten des AG) durchgeführt werden.

4.1 Allgemeines (T2, T3)

Wartungsarbeiten durch den DL erfolgen ausschließlich durch qualifiziertes und geschultes Personal. Die Mitarbeiter sind über die sicherheitstechnischen Anforderungen des AG nachweislich zu schulen, ggf. sind entsprechende Sicherheitsüberprüfungen nachzuweisen.

Alle zur Wartung genutzten Systeme müssen mit einem sicheren logischen Zugangsschutz versehen sein sowie vor einem unberechtigten physischen Zugriff geschützt werden.

Die anderweitige Nutzung von für Wartungsarbeiten genutzten Systemen / Komponenten ist durch den DL zu untersagen. Dies gilt auch für den Fall, dass auf den Systemen eigens für die Wartung installierte virtuelle Maschinen (Betriebssystem und Applikationen) verwendet werden.

4.2 Sichere Systemkonfiguration von Wartungskomponenten (T3)

Für Wartungsarbeiten sind ausschließlich Systeme zu verwenden, die anhand anerkannter Best-Practice-Vorgaben und nach aktuellem Stand der Technik sicher konfiguriert und gehärtet sind.

Die Systeme müssen beim Wartungszugriff über einen aktiven Schadsoftwareschutz, basierend auf aktuellsten AV-Pattern, verfügen.

4.3 Fernwartung (T3)

Fernwartungszugriffe dürfen nur über die vom AG zur Verfügung gestellten Fernwartungszugänge realisiert werden.

Die zur Fernwartung berechtigten Mitarbeiter sind dem AG namentlich mitzuteilen.

Fernwartungszugriffe dürfen auf Seiten des DL nur aus einem nach Stand der Technik gesicherten und gegen unberechtigte Zugriffe geschützten Wartungsnetzwerk erfolgen. Sollen Fernwartungszugriffe direkt von Arbeitsplatzsystemen oder anderen Systemen (z. B. mobile Systeme, Heimarbeitsplatz) erfolgen, muss dies dem AG mitgeteilt und von diesem explizit genehmigt werden.

Fernzugriffe werden auf einem Terminalserver / Jumphost in einer separaten Sicherheitszone des AG terminiert. Der AG legt die technisch / organisatorischen Parameter für die Einwahl fest und übermittelt diese an den DL. Der DL benennt die

für die Wartungsarbeiten benötigten Programme und Tools, welche auf den Systemen bereitgestellt werden müssen, stellt diese zur Installation zur Verfügung und stellt notwendige Aktualisierungen sicher.

Ein direkter Zugriff auf die zu wartenden Systeme des AG unter Umgehung des Terminalservers / Jumphost ist nicht zulässig.

5 Meldung von Informationssicherheitsvorfällen (T1, T2, T3)

Wenn beim DL ein Informationssicherheitsvorfall vorliegt, der Auswirkungen auf die vom DL an den AG gelieferten Produkte oder Dienstleistungen hat oder auf andere Weise die Informationssicherheit des AG gefährdet, ist der DL verpflichtet, den AG unverzüglich darüber zu informieren.

Wenn Zweifel darüber bestehen, ob es sich tatsächlich auch um einen Informationssicherheitsvorfall handelt, muss dies trotzdem gemeldet werden.

Kontaktaufnahme

Hotline Informationssicherheit:	06151-709 8080
E-Mail-Adresse:	lieferantenverpflichtung@e-netz-suedhessen.de
Post-Anschrift:	e-netz Südhessen GmbH & Co. KG Dornheimer Weg 24 64239 Darmstadt