[Name der Organisation]

ST11 Handbuch zur Sicherheit in System- und Netzwerkkonfiguration

Version	*1.0*
Besitzer der Police	Name *eingeben*
Genehmigt durch	Ausschuss *zur Genehmigung der Richtlinie*
Datum der Genehmigung	Datum *eingeben*
Datum des Inkrafttretens	Datum *eingeben*
Nächster Überprüfungstermin	Datum *eingeben*
Vertraulichkeitsstufe	INTERN

Änderungsverlauf

Datum	Version	Erstellt von	Beschreibung der Änderung
17.12.24	0.92	DataGuard	Grundstruktur des Dokuments
XX.XX.24	1.00	XX	Genehmigte Version und minimale Änderungen

[Wie diese DataGuard Richtlinienvorlage zu verwenden ist:]

[DataGuard möchte Ihnen einige wichtige Hinweise zur Anwendung der bereitgestellten Richtlinienvorlage geben. Diese Vorlage soll Ihnen als Ausgangspunkt dienen, um eigene, auf Ihre Organisation zugeschnittene Richtlinien zu entwickeln. Bitte beachten Sie die folgenden Hinweise zur Verwendung der Vorlage sorgfältig.

Verwendung der Vorlage

- **Vorlage als Ausgangspunkt:** Diese Vorlage ist sorgfältig recherchiert und von Experten zusammengestellt worden. Sie ist als Ausgangspunkt für die Erstellung Ihrer eigenen Richtlinie gedacht und bietet eine Struktur sowie Beispiele für Ihre künftiges Dokument. Bei allen Bemühungen erhebt diese Vorlage jedoch keinen Anspruch auf Passgenauigkeit und Vollständigkeit, denn die individuellen Gegebenheiten in Ihrer Organisation können abweichen.
- **Grundsatz der Effektivität:** Eine Richtlinie soll erforderlich, angemessen, passend, aufklärend und unterstützend für Ihren individuellen Unternehmenszweck wirken. Sorgen Sie dafür, dass Ihre Richtlinien stets diesem Grundsatz entsprechen.
- **Überprüfung der Inhalte:** Gehen Sie die Inhalte der Vorlage sorgfältig durch und überprüfen Sie diese im Hinblick auf die spezifischen Bedürfnisse und Anforderungen.
- **Vollständiges Verständnis erforderlich:** Stellen Sie sicher, dass Sie als Ersteller dieses Dokuments alle beschriebenen Anweisungen und Verfahren vollständig verstehen und für Ihre Organisation als anwendbar halten. Nur so können Sie fundierte Entscheidungen über Anpassungen treffen.
- **Klärung von Unklarheiten:** Sollten Sie auf Inhalte stoßen, die Sie nicht vollständig verstehen, holen Sie unbedingt weitere Informationen ein. Dies kann durch Rücksprache mit unseren DataGuard-Experten, rechtlichen Beratern oder anderen Fachexperten außerhalb oder innerhalb Ihrer Organisation geschehen.
- **Individuelle Anpassung erforderlich:** Die in der Vorlage beschriebenen Anweisungen und Verfahren sind pauschale Beispiele oder Vorschläge ohne tiefere Berücksichtigung Ihres Unternehmenskontextes. Daher ist es erforderlich, dass Sie den Inhalt der Richtlinien an die tatsächlichen Gegebenheiten und Anforderungen Ihrer Organisation anpassen.*

- **Keine ungeprüfte Übernahme:** Übernehmen Sie keine Texte oder Anweisungen aus der Vorlage, wenn diese nicht den spezifischen Anforderungen und der tatsächlichen Situation in Ihrer Organisation entsprechen. Jede Organisation ist einzigartig, und pauschale Übernahmen können zu Fehlern oder Missverständnissen führen.
- **Verantwortung der Geschäftsführung:** Beachten Sie, dass die endgültige Verantwortung für die Gestaltung und Umsetzung von Richtlinien bei der obersten Leitung Ihrer Organisation liegt. Es ist entscheidend, dass diese alle Inhalte kritisch überprüft und eine Korrektur von unpassenden Inhalten veranlasst.]

[*) Die in dieser Vorlage gelb hinterlegten und in eckigen Klammern gesetzten Hilfstexte und Hinweise sollen nach Kennnisnahme eliminiert oder inhaltlich angepasst werden. Beispiel: Bitte eliminieren Sie diese Seite vor Veröffentlichung der Richtlinie.]

1 Einleitung

Das Handbuch zur Sicherheit in System- und Netzwerkkonfiguration für[Name der Organisation] stellt einen konsolidierten Rahmen dar, der unsere Strategie für die effektive Konfiguration und den Schutz unserer Systemkonfigurationen und Daten umreißt. Es dient als umfassender Leitfaden, in dem detailliert beschrieben wird, wie die Organisation verschiedene Sicherheitsherausforderungen im Zusammenhang mit der Systemkonfiguration und dem Sicherheit von Daten in unserem gesamten Betrieb angehen wird. Darüber hinaus wird der Ansatz unserer Organisation zur Verwaltung von Systemkonfigurationen und zum Schutz von Daten auf hohem Niveau dargelegt.

1.1 Zweck und Umfang

Das Hauptziel dieser Richtlinie besteht darin, einen strukturierten Ansatz für die Systemkonfiguration und die Sicherheit von Daten zu entwickeln, um die sensiblen Informationen, Vermögenswerte und den Ruf unserer Organisation zu schützen. Durch die Einhaltung dieser Richtlinie wollen wir unsere Widerstandsfähigkeit gegen Sicherheitsverletzungen erhöhen und das Risiko von Datenkompromittierungen oder unbefugtem Zugriff minimieren.

1.2 Anwendbarkeit

Diese Richtlinie gilt für alle Mitarbeiter und Beteiligten und stellt sicher, dass sie die festgelegten Richtlinien für die Systemkonfiguration und die Sicherheit von Daten einhalten. Die IT-Sicherheitsabteilung ist in Zusammenarbeit mit den zuständigen Abteilungen für die Überwachung der Umsetzung, Pflege und kontinuierlichen Verbesserung der in dieser Richtlinie beschriebenen Verfahren verantwortlich.

2 Systemkonfiguration und deren Schutz

2.1 Schutz vor Malware

2.1.1 Richtlinie

Die Organisation muss zum Schutz der Unternehmensdaten vor Malware-Bedrohungen entsprechende Systeme implementieren.

2.1.2 Verfahren

[Bitte beschreiben Sie, wie sich Ihre Organisation vor Malware schützt. Ändern Sie diesen Abschnitt, sofern Sie ein anderes Verfahren in Ihrer Organisation praktizieren. Beachten Sie, dass ein Auditor nach dokumentierten Nachweisen für den beschriebenen Prozess verlangen wird. Seien Sie daher für ein Audit entsprechend vorbereitet und in der Lage, dokumentierte Nachweise für die Durchführung eines solchen Prozesses in einem Audit vorzuzeigen]

Auswahl und Einsatz von Tools zum Schutz vor Malware:

1. Bewerten und wählen Sie geeigneter Software zur Erkennung und Reparatur von Malware auf der Grundlage von Industriestandards, Zuverlässigkeit und Kompatibilität mit bestehenden Systemen aus.

   [Einige Beispiele könnten sein: Die Werkzeuge müssen KI, ML und Angriffsvektorquellen umfassen].

2. Verteilen Sie die Tools zum Schutz vor Malware auf alle relevanten Endgeräte und Server.
3. Konfigurieren Sie die Tools zum Schutz vor Malware entsprechend den bewährten Verfahren und empfohlenen Einstellungen.

Durchführung von Präventivkontrollen:

1. Implementieren Sie Maßnahmen, um die Verwendung von nicht zugelassener Software zu verhindern.[Beispiel: Verwendung von Einstellungen für das Anwendungsrisiko oder automatische Blockierung von bekannter Schadsoftware.]

2. Richten Sie Kontrollen ein, um den Zugriff auf bekannte oder mutmaßlich bösartige Websites mithilfe von Blocklisting-Techniken zu blockieren.

3. Aktualisieren und patchen Sie Software und Systeme regelmäßig, um Schwachstellen zu beseitigen, die von Schadsoftware ausgenutzt werden könnten. [Beispiel: Verwendung von automatischen Updates oder Cloud-Signatur-Tools, z. B. MDR/XDR]

Reaktion auf Zwischenfälle und Wiederherstellung:

1. Leiten Sie nach Erkennen einer Malware-Infektion entsprechend definierte Maßnahmen ein. [Beispiel: Neu-Imaging von Systemen, wenn diese kompromittiert sind].

2. Stellen Sie Daten aus sauberen Backups wieder her, um betroffene Systeme nach einem Malware-Vorfall wieder in einen sicheren Zustand zu versetzen.

2.2 Handhabung von technischen Schwachstellen

2.2.1 Richtlinie

Die Identifizierung, Bewertung und Behebung von technischen Schwachstellen muss umgehend erfolgen, um eine Ausnutzung zu verhindern und die Risiken für die Informationssicherheit zu verringern.

2.2.2 Verfahren

[Dieses Verfahren erläutert, wie die Organisation technische Schwachstellen identifizieren sollte, um die Systeme sicher zu halten und um sie vor Angriffen zu schützen.]

Identifizierung von technischen Schwachstellen:

1. **Bestandsaufnahme der Anlagen:** Führen Sie ein aktuelles Inventar aller Informationssysteme, Software und Komponenten, einschließlich Herstellerangaben, Versionsnummern und zuständigem Personal.

2. **Nutzung von Informationsressourcen:** Überwachen Sie regelmäßig Informationsquellen wie Herstellerhinweise, Sicherheitsbulletins und Schwachstellendatenbanken, um potenzielle Schwachstellen zu identifizieren.

3. **Schwachstellen-Scan-Tools verwenden:** Implementieren Sie automatisierte Tools zum Scannen von Schwachstellen, um die Netzwerkinfrastruktur, Systeme und Anwendungen regelmäßig auf bekannte Schwachstellen zu überprüfen. [DataGuard bietet in seinem Level-2 Plan entsprechende Lösungen an]

4. **Einbindung von Lieferanten:** Arbeiten Sie mit Lieferanten und Anbietern zusammen, um sicherzustellen, dass diese gemäß den vertraglichen Vereinbarungen zeitnah Schwachstellen melden, behandeln und offenlegen.

Berichterstattung und Aufdeckung:

a) Meldung: Nach Erhalt von Schwachstellenmeldungen von internen Beteiligten, externen Analysten und anderen Quellen sollten die Informationen dokumentiert und bewertet werden. [Beispiel: Eröffnen Sie ein Ticket, um die Relevanz und das Risiko zu untersuchen.]

b) Öffentliche Anlaufstelle: Verwenden Sie eine spezielle E-Mail-Adresse oder ein Online-Meldeformular, um die Meldung von Schwachstellen durch externe Beteiligte zu erleichtern. Beispiel: abuse-sec@company.cc

c) Bug Bounty-Programme: Erwägen Sie die Einführung von "Bug Bounty"-Programmen, um Forschern und Sicherheitsinteressierten einen Anreiz zu geben, Schwachstellen zu identifizieren und zu melden und dafür eine Belohnung zu erhalten.

Bewertung der technischen Schwachstellen:

a) Überprüfung und Analyse: Überprüfen und analysieren Sie Schwachstellenberichte, um ihren Schweregrad, ihre Auswirkungen und ihr potenzielles Risiko für die Informationssysteme und Anlagen der Organisation zu bewerten.

b) Penetrationstests: Führen Sie geplante und kontrollierte Penetrationstests oder Schwachstellenbewertungen durch kompetente Einzelpersonen oder Teams durch, um Schwachstellen zu identifizieren, die von automatischen Scanning-Tools nicht erkannt werden.

Behebung technischer Schwachstellen:

a) Patch-Verwaltung: Implementieren Sie einen Patch-Management-Prozess, um genehmigte Patches und Updates für erkannte Schwachstellen rechtzeitig zu priorisieren, zu testen und zu verteilen.

b) Testen von Updates: Testen Sie Patches und Updates gründlich in einer kontrollierten Umgebung, um sicherzustellen, dass sie wirksam sind und keine unerwünschten Nebeneffekte haben.

c) Alternative Kontrollen: Wenn Patches nicht sofort angewendet werden können oder nicht verfügbar sind, sollten Sie alternative Kontrollen wie Netzwerksegmentierung, Zugriffsbeschränkungen oder vorübergehende Umgehungslösungen einführen, um das von den Schwachstellen ausgehende Risiko zu mindern.

d) Verifizierung: Überprüfen Sie die Authentizität und Wirksamkeit der Abhilfemaßnahmen, indem Sie Validierungstests durchführen und das Systemverhalten nach der Implementierung überwachen.

2.3 Konfigurationsmanagement

2.3.1 Richtlinie

Hardware, Software, Dienste und Netzwerke müssen mit gehärteten Sicherheitseinstellungen konfiguriert werden, um Risiken zu minimieren und die Schutzwirksamkeit zu gewährleisten.

2.3.2 Verfahren

[Dieses Verfahren erläutert, wie die Organisation Ihre Geräte so konfiguriert, dass sie ein hohes Maß an Sicherheit bieten, um sie vor Angriffen zu schützen.]

Um sicherzustellen, dass Hardware, Software, Dienste und Netzwerke sicher und konsistent konfiguriert sind und um Risiken zu mindern und die betriebliche Effektivität aufrechtzuerhalten, ist ein systematischer Prozess zur Dokumentation, Implementierung, Überwachung und Überprüfung von Konfigurationen in Übereinstimmung mit der Konfigurationsmanagement-Richtlinie einzurichten.

Technische Sicherheitsstandards:

1. Entwicklung von Standardvorlagen für die sichere Konfiguration von Hardware, Software, Diensten und Netzwerken auf der Grundlage bewährter Branchenverfahren und organisatorischer Anforderungen. [Beispiel: auf der Grundlage von Vorlagen des CIS-Zentrums].
2. Dazu gehören Parameter wie Benutzerzugriffsrechte, Dienstkonfigurationen, Netzwerkeinstellungen und Sicherheitskontrollen.
3. Sicherstellung, dass die Vorlagen regelmäßig überprüft und aktualisiert werden, um neuen Bedrohungen, Schwachstellen oder technologischen Veränderungen Rechnung zu tragen.
4. Einführung eines zentralen Repository für die Konfigurationsdokumentation, einschließlich Konfigurationsvorlagen und Aufzeichnungen über Konfigurationsänderungen.

[Bitte referenzieren Sie hier auf Ihre Konfigurationsdokumentation. Siehe auch Anforderungen in den Richtlinien zum Prozessmanagement (DataGuard Policy-Vorlage ST7)]

Umsetzungsprozess:

1. Implementieren Sie Konfigurationen auf neu eingerichteten Systemen oder bei System-Upgrades nach genehmigten Vorlagen.
2. Befolgen Sie die Verfahren des Änderungsmanagements, um Konfigurationsänderungen anzufordern, zu prüfen und zu genehmigen.
3. Dokumentieren Sie alle Konfigurationsänderungen, einschließlich des Grundes für die Änderung, des Genehmigungsstatus und der Implementierungsdetails.

Überwachung und Überprüfung:

1. Regelmäßige Überwachung der Konfigurationen mit Hilfe von Systemmanagement-Tools, um die Einhaltung der festgelegten Vorlagen zu gewährleisten.
2. Regelmäßige Überprüfung der Konfigurationseinstellungen anhand von Zielvorlagen, um Abweichungen oder Nichteinhaltung zu ermitteln.

3. Untersuchung und Beseitigung von Unstimmigkeiten durch automatische Durchsetzung oder manuelle Korrekturmaßnahmen.

Integration und Automatisierung:

1. Integration von Konfigurationsmanagementprozessen mit Asset-Management-Systemen und anderen relevanten Tools zur Rationalisierung der Abläufe.

2. Prüfung von Automatisierungsoptionen, wie z. B. Infrastruktur als Code, um die Bereitstellung und Durchsetzung von Konfigurationen zu automatisieren.

2.4 Synchronisierung der Systemuhrzeit

2.4.1 Richtlinie

Die Uhren von Informationsverarbeitungssystemen müssen mit zugelassenen Zeitquellen synchronisiert werden, um die Korrelation und Analyse von sicherheitsrelevanten Ereignissen und anderen aufgezeichneten Daten zu ermöglichen und Untersuchungen von Informationssicherheitsvorfällen zu unterstützen.

2.4.2 Verfahren

[Dieses Verfahren erklärt, wie die Organisation sicherstellt, dass alle Uhren aller Systeme im Geltungsbereich synchronisiert sind. Dies ist aus den folgenden Gründen wichtig:

- Die Uhrensynchronisation gewährleistet genaue Zeitstempel für Sicherheitsmechanismen wie Authentifizierung, Protokollierung und Sitzungsverwaltung.
- Es verhindert Replay-Angriffe, indem es die Zeit zwischen den kommunizierenden Parteien konsistent hält.
- Genaue Zeitstempel helfen bei der forensischen Analyse und Untersuchung von Sicherheitsvorfällen.
- Inkonsistente Uhren können zu Schwachstellen bei kryptografischen Operationen führen und die Sicherheitsgarantien schwächen.
- Die Synchronisierung ist entscheidend für die Koordinierung und die Datenkonsistenz in verteilten Systemen].

Rollen & Zuständigkeiten: [ändern Sie diese, wenn Sie andere Rollen oder Zuständigkeiten haben]

1. IT-Administarionsteam: Verantwortlich für die Überwachung der Implementierung und Wartung der Zeitsynchronisation zwischen den Informationsverarbeitungssystemen.

2. Systemadministratoren: Verantwortlich für die Konfiguration der einzelnen Systeme zur Synchronisierung ihrer Uhren mit zugelassenen Zeitquellen.

3. IT-Sicherheitsteam: Verantwortlich für die Überwachung und Überprüfung der Einhaltung der Zeitsynchronisationsanforderungen.

Verfahren:

Identifizierung der genehmigten Zeitquellen:

- Das IT-Administrationsteam identifiziert und genehmigt zuverlässige Zeitquellen, wie nationale Atomuhren, GPS-Zeitübertragungen oder andere maßgebliche Zeitserver. [Beispiel: Google NTP, Cloudflake NTP, Microsoft NTP, Apple NTP]

Konfiguration der Referenzuhr:

- Eine Uhr, die mit einer genehmigten Zeitquelle verbunden ist, wird als Referenzuhr für Protokollierungssysteme bezeichnet.
- Die Referenzuhr ist so konfiguriert, dass sie Zeitaktualisierungen von der zugelassenen Zeitquelle über Protokolle wie NTP oder PTP empfängt.

Synchronisierung von Informationsverarbeitungssystemen:

- Die Systemadministratoren konfigurieren die einzelnen Informationsverarbeitungssysteme so, dass ihre Uhren mit der Referenzuhr synchronisiert werden.
- Die Einstellungen für Network Time Protocol (NTP) oder Precision Time Protocol (PTP) werden auf jedem System

konfiguriert, um eine genaue Zeitsynchronisation zu gewährleisten.

- Die Synchronisierungshäufigkeit und die Abfrageintervalle werden auf der Grundlage von organisatorischen Anforderungen und bewährten Verfahren festgelegt.

Überwachung und Verifizierung:

- Das Sicherheitsteam führt regelmäßige Kontrollen durch, um zu überprüfen, ob alle Informationsverarbeitungssysteme mit den genehmigten Zeitquellen synchronisiert sind.
- Automatisierte Tools können zur Überwachung des Zeitsynchronisationsstatus in der gesamten Infrastruktur des Unternehmens eingesetzt werden.
- Abweichungen oder Unstimmigkeiten bei der Zeitsynchronisation werden umgehend untersucht und behoben.

2.5 Verwendung von Hilfsprogrammen mit privilegierten Rechten

2.5.1 Richtlinie

Der Zugriff auf Hilfsprogramme, mit denen System- und Anwendungsschutzmaßnahmen außer Kraft gesetzt werden können, darf nur befugten Personen gewährt werden, die im Rahmen ihrer beruflichen Tätigkeit einen legitimen Bedarf für diesen Zugriff haben.

2.5.2 Verfahren

[Dieses Verfahren erklärt, wie die Organisation den Zugang zu bestimmten Dienstprogrammen (die oft die administrative Kontrolle über andere Systeme haben) verwalten wird.]

Identifizierung von Hilfsprogrammen:

1. Überprüfen Sie alle Systeme und Anwendungen, um Hilfsprogramme zu identifizieren, die in der Lage sind, System- und Anwendungssteuerungen außer Kraft zu setzen.
2. Dokumentieren Sie die Liste der identifizierten Hilfsprogramme zusammen mit deren Fähigkeiten.

Autorisierung und Zugriffskontrolle:

1. Bestimmen Sie die Mindestanzahl der autorisierten Benutzer, die aufgrund ihrer Aufgaben und Zuständigkeiten Zugriff auf Versorgungsprogramme benötigen.
2. Implementieren Sie Verfahren zur Benutzeridentifizierung, Authentifizierung und Autorisierung für den Zugriff auf Versorgungsprogramme.
3. Weisen Sie jedem Benutzer, der auf Dienstprogramme zugreift, eindeutige Identitäten zu.
4. Definieren und dokumentieren Sie Berechtigungsstufen, die festlegen, wer auf Hilfsprogramme zugreifen, und diese nutzen darf.
5. Sorgen Sie für die Einholung von Genehmigungen der Geschäftsführung für die Ad-hoc-Nutzung von Dienstprogrammen.

Abtrennung und Abschaffung unnötiger Programme:

1. Trennen Sie Dienstprogramme von Anwendungssoftware, um Störungen des normalen Systembetriebs zu vermeiden.
2. Entfernen oder deaktivieren Sie alle unnötigen Hilfsprogramme von den Systemen, um die potenzielle Angriffsfläche zu minimieren.

Protokollierung und Überwachung:

1. Implementieren Sie Protokollierungsmechanismen zur Aufzeichnung der gesamten Nutzung von Hilfsprogrammen, einschließlich Benutzeridentifikation und durchgeführter Aktionen.
2. Überwachen Sie die Protokolle regelmäßig, um jede unbefugte oder verdächtige Nutzung von Hilfsprogrammen zu erkennen.

Begrenzte Verfügbarkeit und Dauer:

1. Beschränken Sie die Verfügbarkeit von Hilfsprogrammen auf autorisierte Benutzer.

2. Gewähren Sie nur für die Dauer von genehmigten Änderungen oder Wartungsarbeiten Zugang zu den Dienstprogrammen.

Schulung und Sensibilisierung:

1. Veranlassen Sie Schulungen autorisierter Benutzer in der ordnungsgemäßen Verwendung von Hilfsprogrammen und der Einhaltung von Unternehmensrichtlinien und -verfahren.
2. Sensibilisieren Sie Benutzer für die Bedeutung einer eingeschränkten und kontrollierten Nutzung von Hilfsprogrammen für die Informationssicherheit.

Regelmäßige Überprüfung und Aktualisierung:

1. Es muss eine regelmäßige Überprüfung und Aktualisierung der Liste der autorisierten Benutzer und Dienstprogramme auf der Grundlage organisatorischer Änderungen und Anforderungen erfolgen.
2. Die Durchführung regelmäßiger Audits, um die Einhaltung der Richtlinie zu gewährleisten und verbesserungswürdige Bereiche zu ermitteln muss sichergestellt werden.

[Bitte berücksichtigen sie die Audits in Ihrem Management von Informationssicherheitsaufgaben]

2.6 Installation von Software auf betrieblichen Systemen

2.6.1 Richtlinie

Um die Integrität der operativen Systeme zu gewährleisten und die Ausnutzung technischer Schwachstellen zu verhindern, muss das Unternehmen die Softwareinstallation kontrollieren und verwalten.

2.6.2 Verfahren

[Überprüfen Sie dieses Verfahren, um sicherzustellen, dass es mit den Prozessen Ihrer Organisation übereinstimmt. In diesem Verfahren wird erläutert, wie Ihre Organisation die Installation von Betriebssystemsoftware verwaltet; dies ist eine wichtige Maßnahme und umfasst viele Schritte, von der Genehmigung einer bestimmten Betriebssystemsoftware bis hin zur Verwaltung von Protokollen. Es wird empfohlen, dass Sie mindestens alle unten aufgeführten Schritte durchführen]

Autorisierung und Personalschulung:

1. Nur IT-Administratoren mit entsprechender Berechtigung dürfen Softwareinstallationen oder -aktualisierungen auf operativen Systemen durchführen.
2. Die Geschäftsleitung muss bestimmte Mitarbeiter aufgrund ihrer Ausbildung und Erfahrung für diese Aufgabe autorisieren.

Genehmigungsverfahren:

1. Vor jeder Softwareinstallation oder -aktualisierung müssen die Administratoren die Genehmigung des zuständigen Verwaltungspersonals einholen.
2. Es wird ein förmliches Genehmigungsverfahren eingeführt, das die erforderlichen Schritte zur Beantragung und Genehmigung von Softwareänderungen festlegt.

Prüfung und Validierung:

1. Software-Installationen und -Updates müssen umfangreiche Tests und Validierungen durchlaufen, um Kompatibilität, Funktionalität und Sicherheit zu gewährleisten.
2. Die Testumgebungen müssen die Produktionssysteme so genau wie möglich widerspiegeln, um die Auswirkungen von Softwareänderungen genau beurteilen zu können.

Identifizierung von genehmigtem ausführbarem Code:

1. Führen Sie eine Liste von genehmigtem ausführbarem Code, der zur Installation auf operativen Systemen zugelassen ist.
2. Nur Software aus vertrauenswürdigen und überprüften Quellen soll in diese Liste aufgenommen werden.

Konfigurationskontrolle:

1. Verwendung eines Konfigurationskontrollsystems zur Verwaltung und Verfolgung aller Softwareinstallationen und -

aktualisierungen auf den operativen Systemen.

2. Dieses System muss eine Aufzeichnung der vorgenommenen Änderungen mit Versionsnummern, Datum und Gründen für die Änderung führen.

Rollback-Strategie:

1. Entwickeln Sie eine Rollback-Strategie, um im Falle einer fehlgeschlagenen Softwareinstallation oder -aktualisierung den vorherigen Zustand wiederherzustellen.

2. Dokumentieren Sie das Rollback-Verfahren und stellen Sie sicher, dass die Administratoren darin geschult werden, wie es effektiv ausgeführt werden kann.

Audit-Protokollierung:

1. Aktivieren Sie die Protokollierung aller Software-Installations- und Aktualisierungsaktivitäten auf operativen Systemen.

2. Die Protokolleinträge müssen Einzelheiten wie Datum und Uhrzeit der Änderung, die installierte oder aktualisierte Software und den zuständigen Administrator enthalten.

Alte Versionen archivieren:

1. Führen Sie ein Repository alter Softwareversionen zusammen mit der entsprechenden Dokumentation und den Konfigurationsdetails.

2. Archivierte Versionen sind so lange aufzubewahren, wie sie für Referenzzwecke oder die Einhaltung von Vorschriften benötigt werden.

Unterstützung von Anbietern und Open-Source-Wartung:

1. Prüfen Sie regelmäßig, ob von den Softwareherstellern Updates und Patches für unterstützte Versionen zur Verfügung gestellt werden.

2. Überwachen Sie den Wartungsstatus von Open-Source-Software, die in operativen Systemen verwendet wird, und aktualisieren Sie sie bei Bedarf auf die jeweils neueste Version.

Überwachung extern bereitgestellter Software:

1. Überwachen Sie extern bereitgestellte Software und Pakete auf nicht autorisierte Änderungen, die Sicherheitslücken verursachen könnten.

2. Regelmäßige Überprüfung der Integrität extern gelieferter Software, um sicherzustellen, dass sie mit den Sicherheitsstandards der Organisation übereinstimmt.

Zugang und Überwachung von Lieferanten:

1. Gewähren Sie Lieferanten nur dann Zugang zur Installation oder Aktualisierung von Software, wenn dies erforderlich ist und eine entsprechende Genehmigung vorliegt.

2. Überwachen Sie Aktivitäten der Zulieferer bei Softwareänderungen, um die Einhaltung der Unternehmensrichtlinien und -verfahren zu gewährleisten.

Regeln für die Installation von Anwendersoftware:

1. Setzen Sie strenge Regeln für vom Benutzer installierte Software auf operativen Systemen durch.

2. Geben Sie den Nutzern klare Richtlinien an die Hand, welche Softwareinstallationen erlaubt und welche verboten sind.

Grundsatz der geringsten Privilegierung (least Privilege):

1. Wenden Sie das Prinzip der geringsten Rechte bei der Vergabe von Berechtigungen für Software-Installationen auf operativen Systemen an.

2. Beschränken Sie die Installationsrechte auf die Rechte, die erforderlich sind, damit die Benutzer ihre Aufgaben effektiv erfüllen können.

3 Netzwerke und Informationsübertragung

3.1 Informationsübertragung

3.1.1 Richtlinie

Alle Informationen müssen sicher übertragen werden, um eine wirksame Verwaltung, Überwachung und den Schutz von Informationsbeständen zu ermöglichen. Das Personal muss die verschiedenen Arten von Informationen gemäß dieser Richtlinie unter Beachtung der Regeln, Verfahren und Vereinbarungen für die Datenklassifizierung der betreffenden Informationen behandeln.

Übertragungsvereinbarungen:

Erstellen Sie Übertragungsvereinbarungen (einschließlich Authentifizierung des Empfängers) zum Schutz von Informationen aller Art bei der Übermittlung zwischen dem Unternehmen und Dritten und erhalten Sie diese aufrecht.

3.1.2 Verfahren

[Dieses Verfahren erläutert, wie die Organisation mit der Übermittlung von Informationen umgeht; dies gilt sowohl für digitale als auch für physische Medien (wie Festplatten) sowie für mündliche Informationen (wenn sensible Daten laut ausgesprochen werden)].

Grundlegende Überlegungen zur Übermittlung von Informationen durch elektronische Mittel, physische Speichermedien und mündliche Kommunikation.

Elektronischer Transfer:

- **Schutz vor Malware:**
  Erkennung und Schutz vor Malware, die durch elektronische Kommunikation übertragen wird.
- **Pfändungsschutz:**
  Schutz sensibler elektronischer Informationen in Anhängen.
- **Überprüfung der Adresse:**
  Verhindern des Versands von Dokumenten und Nachrichten an eine falsche Adresse oder Nummer.
- **Genehmigung für externe Dienstleistungen:**

  Einholung von Genehmigungen, bevor externe öffentliche Dienste wie Instant Messaging, soziale Netzwerke, Dateifreigabe oder Cloud-Speicher genutzt werden dürfen.
- **Authentifizierung:**
  Einführung stärkerer Authentifizierungsstufen für Übertragungen über öffentlich zugängliche Netze.
- **Beschränkungen der Kommunikation:**

  Beschränkungen für elektronische Kommunikationseinrichtungen festlegen, um Probleme wie die automatische Weiterleitung von E-Mails an externe Adressen zu verhindern.
- **Hinweise zu SMS und Instant Messages:**

  Hinweisen des Personals darauf, keine kritischen Informationen über SMS oder Sofortnachrichten zu versenden, da diese an öffentlichen Orten gelesen oder in unzureichend geschützten Geräten gespeichert werden können.
- **Bedenken gegen Faxgeräte:**

  Information des Personals über die Probleme bei der Nutzung von Faxgeräten oder -diensten, wie z. B. den unbefugten Zugriff auf Nachrichtenspeicher und die absichtliche oder versehentliche Programmierung von Geräten.

Übertragung physischer Speichermedien:

- **Zuständigkeiten:**
  Legen Sie die Zuständigkeiten für die Kontrolle und Benachrichtigung von Übermittlung, Versand und Empfang fest.
- **Adressierung und Transport:**

  Stellen Sie die korrekte Adressierung und Beförderung von Nachrichten sicher.
- **Verpackung:**

  Verwenden von Verpackungen, die den Inhalt vor physischen Schäden während des Transports schützt.
- **Identifizierung des Kuriers:**

  Festlegung von Standards für die Identifizierung von Kurieren.

- **Manipulationssichere Übertragungsmaßnahmen:**

  Je nach Geheimhaltungsgrad der Informationen sind manipulationssichere oder manipulationssichere Übertragungsmaßnahmen zu verwenden.

- **Zugelassene Drittparteien:**

  Führen Sie eine genehmigte Liste von Dienstleistern, die Transport- oder Kurierdienste für Sie durchführen dürfen.

- **Protokolle:**

  Führen Sie Protokolle, aus denen der Inhalt der Speichermedien, der angewandte Schutz, die autorisierten Empfänger und die Übertragungszeiten hervorgehen.

Mündliche Übertragung:

- **Öffentliche Konversationen:**
  Weisen Sie das Personal darauf hin, keine vertraulichen Gespräche an öffentlichen Orten oder über unsichere Kommunikationskanäle zu führen.

- **Sprachnachrichten:**

  Achten Sie darauf, keine Nachrichten mit vertraulichen Informationen auf Anrufbeantwortern oder Sprachnachrichten zu hinterlassen.

- **Screening:**
  Stellen Sie sicher, dass die Personen auf die für das Anhören des Gesprächs geeignete Stufe überprüft werden.

- **Zimmerkontrollen:**

  Führen Sie geeignete Raumkontrollen durch, wie z. B. Schalldämmung und geschlossene Türen.

- **Haftungsausschlüsse:**
  Vor dem Beginn sensibler Gespräche ist es wichtig, die Beteiligten auf Sicherheitsmaßnahmen und Vertraulichkeit hinzuweisen. Dadurch wird sichergestellt, dass sich alle Teilnehmer der Vertraulichkeit des Gesprächs bewusst sind und wissen, wie die Informationen, die sie erhalten werden, zu behandeln sind.

3.2 Sicherheit der Netze

3.2.1 Richtlinie

Netze müssen unter Berücksichtigung der Sicherheit konzipiert werden, einschließlich des Einsatzes von Firewalls, Systemen zur Erkennung von Eindringlingen, sicherer Verwaltung und Konfigurationen für alle Netzgeräte.

3.2.2 Verfahren

[Dieses Verfahren erläutert, wie die Netzwerkverwaltung und -konfiguration durchgeführt wird, angefangen bei der Implementierung technischer Netzwerkmaßnahmen (z. B. Firewalls) bis hin zur korrekten Protokollierung und Speicherung des Netzwerkverkehrs. Ändern Sie diesen Abschnitt, sofern Sie ein anderes Verfahren in Ihrer Organisation praktizieren. Beachten Sie, dass ein Auditor nach dokumentierten Nachweisen für den beschriebenen Prozess verlangen wird. Seien Sie daher für ein Audit entsprechend vorbereitet und in der Lage, dokumentierte Nachweise für die Durchführung eines solchen Prozesses in einem Audit vorzuzeigen]

Klassifizierung von Informationen:

1. Identifizieren und klassifizieren Sie die Art und den Empfindlichkeitsgrad der Informationen, die das Netzwerk durchlaufen.

2. Sorgen Sie für die Festlegung geeigneter Sicherheitsmaßnahmen auf der Grundlage der Klassifizierung.

Festlegung von Zuständigkeiten und Verfahren:

1. Benennen Sie verantwortliche Personen oder Teams für die Verwaltung der Netzwerkausrüstung und -geräte.

2. Entwickeln und dokumentieren Sie Verfahren für die Konfiguration, Überwachung und Wartung von Netzsicherheitskontrollen.

Dokumentation und Wartung:

1. Führung einer aktuellen Dokumentation, einschließlich Netzwerkdiagrammen, Inventar von Netzwerkgeräten und Konfigurationsdateien.
2. Regelmäßige Überprüfung und Aktualisierung der Netzdokumentation, um Änderungen der Konfigurationen oder der Netztopologie zu berücksichtigen.
   [Bitte referenzieren Sie hier auf Ihre Konfigurationsdokumentation]

Durchführung von Sicherheitsmaßnahmen:

1. Einsatz von Sicherheitsmaßnahmen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der über das Netz übertragenen Daten.
2. Konfiguration von Firewalls, Intrusion Detection/Prevention-Systeme und Zugriffskontrolllisten (ACLs), um den unbefugten Zugriff auf Netzwerkressourcen zu beschränken.
3. Sicherstellung des Vorhandenseins von geeigneten Authentifizierungsmechanismen, um die Identität von Systemen, die sich mit dem Netz verbinden, zu überprüfen.

Protokollierung und Überwachung:

1. Aktivierung von Protokollierungs- und Überwachungsfunktionen auf Netzwerkgeräten, um den Netzwerkverkehr, Systemaktivitäten und Sicherheitsereignisse aufzuzeichnen.
2. Implementierung einer zentralisierten Protokollierungslösung, um Protokolle aus der gesamten Netzwerkinfrastruktur zu sammeln und zu analysieren.

Netzsegmentierung und -isolierung:

1. Segmentierung des Netzes in logische Zonen auf der Grundlage von Sicherheitsanforderungen und Zugangskontrollen.
2. Isolieren von kritischen Teilnetzen oder sensiblen Systemen, um unbefugten Zugriff oder seitliche Bewegungen von Angreifern zu verhindern.

Schwachstellen-Management:

1. Regelmäßiges Scannen des Netzwerks auf Schwachstellen mit automatischen Tools oder manuellen Bewertungen.
2. Rechtzeitige Behebung von Schwachstellen, die bei Scans festgestellt wurden, um das Risiko eines Missbrauchs zu verringern.

3.3 Sicherheit der Netzdienste

3.3.1 Richtlinie

Die sichere Nutzung von Netzdiensten innerhalb der Organisation muss durch die Ermittlung, Umsetzung und Überwachung geeigneter Sicherheitsmechanismen, Dienstgüteklassen und Dienstanforderungen gewährleistet werden.

3.3.2 Verfahren

[Dieses Verfahren erläutert, wie die Organisation bestimmte Dienste, die über das Netz genutzt werden, verwaltet und pflegt; dies reicht vom Zugang zu bestimmten Netzen bis hin zur Nutzung von VPNs. Ändern Sie diesen Abschnitt, sofern Sie ein anderes Verfahren in Ihrer Organisation praktizieren. Beachten Sie, dass ein Auditor nach dokumentierten Nachweisen für den beschriebenen Prozess verlangen wird. Seien Sie daher für ein Audit entsprechend vorbereitet und in der Lage, dokumentierte Nachweise für die Durchführung eines solchen Prozesses in einem Audit vorzuzeigen].

Identifizierung von Sicherheitswerten:

1. Bewertung der Sicherheitsanforderungen für jeden in der Organisation genutzten Netzdienst.
2. Bestimmung der erforderlichen Sicherheitsmerkmale, Service-Levels und Serviceanforderungen auf der Grundlage der Sensibilität der Daten und der Kritikalität der Dienste.
3. Dokumentation der ermittelten Sicherheitsmaßnahmen für jeden Netzdienst im Detail.

Durchführung von Sicherheitsmaßnahmen:

1. Zusammenarbeit mit internen oder externen Netzdienstleistern, um die Umsetzung der ermittelten Sicherheitsmaßnahmen zu gewährleisten.

2. Weitergabe klarer Anweisungen und Anforderungen an Dienstleister in Bezug auf die zu implementierenden Sicherheitsmerkmale, Servicelevel und Serviceanforderungen.
3. Überwachung des Implementierungsprozesses, um die Einhaltung der vereinbarten Sicherheitsmaßnahmen zu gewährleisten.

Formulierung von Regeln für die Nutzung von Netzen und Diensten:

1. Entwicklung von Regeln und Richtlinien für die Nutzung von Netzen und Netzdiensten innerhalb der Organisation.
2. Definition von Richtlinien für Authentifizierung, Autorisierung, Netzwerkmanagement und Zugangskontrollen.
3. Festlegung von zulässigen Mittel für den Zugriff auf Netzwerke und Dienste, einschließlich VPN-Nutzung und drahtlose Netzwerkverbindungen.
4. Festlegung von Verfahren zur Überwachung der Nutzung von Netzdiensten und zur Durchsetzung der Einhaltung von Nutzungsrichtlinien.

Integration von Sicherheitsfunktionen in Netzwerkdienste:

1. Koordinierung mit Netzwerkadministratoren und Dienstanbietern, um Sicherheitsfunktionen effektiv in Netzwerkdienste zu integrieren.
2. Sicherstellung, dass Authentifizierungsmechanismen, Verschlüsselungsprotokolle und Zugriffskontrollen ordnungsgemäß konfiguriert und durchgesetzt werden.
3. Konfiguration von Netzwerkverbindungsverfahren und Caching-Parameter entsprechend den Sicherheitsanforderungen.
4. Implementierung von Verfahren zur Beschränkung des Zugangs zu sensiblen Netzdiensten oder Anwendungen auf der Grundlage vordefinierter Kriterien.

Überwachung und Bewertung:

1. Regelmäßige Überwachung der Leistung und Sicherheit der Netzdienste, um Abweichungen von den festgelegten Sicherheitsmaßnahmen festzustellen.
2. Durchführung regelmäßiger Überprüfungen und Audits, um die Einhaltung der Sicherheitsrichtlinien und -vorschriften zu gewährleisten.
3. Bewertung der Wirksamkeit der eingeführten Sicherheitsmaßnahmen und gegebenenfalls Anpassung an neue Bedrohungen oder Schwachstellen.

Dokumentation und Berichterstattung:

1. Detaillierte Dokumentation der für jeden Netzdienst implementierten Sicherheitsmaßnahmen, einschließlich Konfigurationseinstellungen und Zugangskontrollen.
2. Erstellung regelmäßiger Berichte über den Sicherheitsstatus von Netzdiensten, einschließlich der Einhaltung der Sicherheitsrichtlinien und aller festgestellten Risiken oder Vorfälle.
3. Zugang zu Sicherheitsdokumenten und -berichten für die relevanten Interessengruppen, um Transparenz und Rechenschaftspflicht zu gewährleisten.

3.4 Trennung von Netzen

3.4.1 Richtlinie

Um die Sicherheit zu erhöhen, den Datenverkehr entsprechend den geschäftlichen Erfordernissen zu steuern und sensible Informationen zu schützen, muss eine Netzwerktrennung vorgenommen werden.

3.4.2 Verfahren

[Dieses Verfahren regelt, wie Ihre Organisation Netzwerke abtrennt, um sie im Falle einer Kompromittierung zu isolieren. Ändern Sie diesen Abschnitt, sofern Sie ein anderes Verfahren in Ihrer Organisation praktizieren. Beachten Sie, dass ein Auditor nach dokumentierten Nachweisen für den beschriebenen Prozess verlangen wird. Seien Sie daher für ein Audit entsprechend vorbereitet und in der Lage, dokumentierte Nachweise für die Durchführung eines solchen Prozesses in einem Audit vorzuzeigen].

Zuständigkeiten:

IT-Abteilung:

- Verantwortlich für die Umsetzung und Aufrechterhaltung von Maßnahmen zur Netztrennung.
- Durchführung regelmäßiger Audits und Bewertungen, um die Einhaltung der Richtlinie zu gewährleisten.
- Bereitstellung von technischer Unterstützung und Hilfe bei der Umsetzung der Netzwerktrennung.

Abteilungsleiter/Manager:

- Zusammenarbeit mit der IT-Abteilung bei der Festlegung von Netzwerkdomänen auf der Grundlage von Geschäftsanforderungen.
- Sicherstellen, dass die IT-Abteilung über Zugangsanforderungen und Sicherheitsaspekte informiert wird.

Verfahren:

Identifizieren Sie Netzwerkdomänen:

- Zusammenarbeit mit Abteilungsleitern und Managern, um die Netzwerkdomänen auf der Grundlage von Geschäftsbereichen, Sensibilität, Kritikalität oder anderen relevanten Faktoren zu ermitteln.
- Dokumentieren Sie die ermittelten Netzwerkdomänen und die damit verbundenen Anforderungen.

Definieren Sie die Begrenzungen für jeden Bereich:

- Arbeiten Sie mit der IT-Abteilung zusammen, um die Grenzen für jede Netzwerkdomäne festzulegen.
- Bestimmen Sie die Zugangskontrollmechanismen, wie Firewalls oder Filterrouter, die an der Peripherie implementiert werden sollen.

Trennen Sie WLAN-Netzwerke:

- Bewerten Sie drahtlose Netzinfrastruktur des Unternehmens und legen Sie geeignete Trennungsmaßnahmen z.B. von internen und Gäste-WLAN fest.
- Passen Sie die Funkabdeckung an, um WLAN-Netzwerke abzutrennen und Zugangskontrollen einzurichten.
- Behandeln Sie WLAN-Verbindungen als externe Verbindung, solange sie kein Gateway in Übereinstimmung mit den Netzwerkschutzmaßnahmen passiert hat.

Durchführung von Schutzmaßnahmen:

- Stellen Sie die Bereitstellung der erforderlichen Hardware- und Softwarelösungen zur Umsetzung der Netzwerktrennungsmaßnahmen zur Verfügung.
- Konfigurieren Sie Firewalls, Router und andere Sicherheitsgeräte, um Zugriffskontrollrichtlinien zwischen Netzwerkdomänen durchzusetzen.
- Stellen Sie sicher, dass die Maßnahmen zur Trennung von drahtlosen Netzen ordnungsgemäß konfiguriert und getestet werden.

Schulung und Sensibilisierung:

- Schuluen und Sensibilisieren Sie Mitarbeiter für die Bedeutung der Netztrennung und die Auswirkungen auf die Sicherheit.
- Klären Sie Mitarbeiter auf über ihre Aufgaben und Verantwortlichkeiten bei der Aufrechterhaltung der Netzsicherheit.

Überwachung und Wartung:

- Richten Sie Überwachungsmechanismen zur kontinuierlichen Beobachtung des Netzwerkverkehrs und zur Identifizierung unberechtigter Zugriffsversuche ein.
- Sorgen Sie für regelmäßige Wartung der Netzwerktrennungskontrollen, um deren Wirksamkeit zu gewährleisten.
- Beheben Sie festgestellte Probleme oder Schwachstellen unverzüglich.

Dokumentation und Berichterstattung:

- Dokumentieren Sie Maßnahmen zur Netztrennung, einschließlich Konfigurationen, Richtlinien und Verfahren.

- Erstellen Sie regelmäßige Berichte über die Einhaltung der Netzwerktrennung und über Sicherheitsvorfälle zur Überprüfung durch das Management.

4 Protokollierung, Überwachung und Web-Filterung

4.1 Verhinderung von Datenverlusten

4.1.1 Richtlinie

Zum Schutz sensibler Daten müssen Maßnahmen zur Aufdeckung und Verhinderung der unbefugten Offenlegung und Extraktion sensibler Informationen ergriffen werden.

4.1.2 Verfahren

[In diesem Verfahren wird erläutert, wie Sie das Risiko von Datenlecks handhaben. Dies reicht von Präventionsmaßnahmen (wie DLP-Tools) bis hin zu Methoden der Datensicherung. Ändern Sie diesen Abschnitt, sofern Sie ein anderes Verfahren in Ihrer Organisation praktizieren. Beachten Sie, dass ein Auditor nach dokumentierten Nachweisen für den beschriebenen Prozess verlangen wird. Seien Sie daher für ein Audit entsprechend vorbereitet und in der Lage, dokumentierte Nachweise für die Durchführung eines solchen Prozesses in einem Audit vorzuzeigen].

Identifizierung und Klassifizierung von sensiblen Informationen:

1. Die Geschäftsleitung oder benannte Asset Eigentümer sind für die Identifizierung und Klassifizierung sensibler Informationen auf der Grundlage ihrer Art und der potenziellen Auswirkungen ihrer Weitergabe verantwortlich.
2. Die Durchführung wiederkehrender Datenklassifizierungsverfahren mit den Asset-Eigentümern ist sicherzustellen.
3. Vergewissern Sie sich, dass die Klassifizierung im Asset-Verzeichnis der Organisation korrekt hinzugefügt wurde.

Überwachung von Anzeichen von Datenlecks:

1. Implementieren Sie Mechanismen zur Überwachung des Datenflusses in den verschiedenen Kanälen, einschließlich E-Mail, Dateitransfer, mobile Geräte und mobile Speichermedien.
2. Setzen Sie Tools zur Verhinderung von Datenlecks zur kontinuierlichen Überwachung von Datenübertragungs- und -zugriffsmustern ein, um potenzielle Datenlecks zu erkennen.
3. Richten Sie Warnungen und Benachrichtigungen ein, um Administratoren umgehend über verdächtige Aktivitäten oder unbefugte Versuche, auf sensible Daten zuzugreifen oder sie zu übertragen, zu informieren.

Präventionsmaßnahmen:

1. Setzen Sie DLP-Tools (Data Leakage Prevention) zur proaktiven Erkennung ein und blockieren Sie unbefugte Versuche, auf sensible Informationen zuzugreifen, sie zu übertragen oder offenzulegen.
2. Konfigurieren Sie DLP-Lösungen, um Richtlinien durchzusetzen, die Datenverluste über E-Mail, File-Sharing-Plattformen, Messaging-Apps und andere Kommunikationskanäle verhindern.
3. Implementieren Sie Maßnahmen, um E-Mails, Dateien oder Nachrichten mit sensiblen Informationen unter Quarantäne zu stellen oder zu blockieren, bevor sie das Netzwerk des Unternehmens verlassen.

Benutzerbeschränkungen und Rechenschaftspflicht:

1. Bewerten Sie die Rollen und Zuständigkeiten der Benutzer, um den Grad des Zugriffs und der Berechtigungen zu bestimmen, der für die Ausführung der Arbeitsfunktionen erforderlich ist.
2. Schränken Sie die Möglichkeiten der Benutzer zum Kopieren, Einfügen oder Übertragen sensibler Informationen auf externe Geräte oder Cloud-Dienste entsprechend ihren beruflichen Anforderungen und ihrer Sicherheitsfreigabe ein.
3. Implementieren Sie Mechanismen zur Benutzerauthentifizierung und Prüfprotokolle, um Benutzeraktionen zu verfolgen und Personen für unbefugten Datenzugriff oder -weitergabe zur Verantwortung zu ziehen.

Steuerungen für Bildschirmaufnahmen und Fotografie:

1. Verbieten Sie Mitarbeitern, Screenshots oder Fotos von sensiblen Informationen ohne entsprechende Genehmigung anzufertigen.
2. Informieren Sie Ihre Mitarbeiter über die Risiken, die mit der Erfassung sensibler Daten verbunden sind, und über die

Folgen eines Verstoßes gegen die Richtlinien zur Verhinderung von Datenverlusten.

3. Überwachen Sie Benutzeraktivitäten und Bildschirmaufnahmen, um Richtlinienverstöße oder Sicherheitsverletzungen zu erkennen und zu untersuchen.

Schutz von Sicherungsdaten:

1. Stellen Sie sicher, dass Sicherungssysteme und Speichermedien, die sensible Informationen enthalten, angemessen vor unbefugtem Zugriff oder Manipulation geschützt sind.

2. Verschlüsseln Sie Sicherungsdaten, um eine unbefugte Offenlegung zu verhindern und die Einhaltung von Sicherheit von Datenbestimmungen zu gewährleisten.

3. Testen Sie regelmäßig Sicherungs- und Wiederherstellungsverfahren, um die Integrität und Sicherheit der gespeicherten Daten zu überprüfen.

4.2 Protokollierung

4.2.1 Richtlinie

Eine effektive Verwaltung von Protokollen, die Aktivitäten, Ausnahmen, Fehler und andere relevante Ereignisse in den Informationssystemen und Netzwerken des Unternehmens aufzeichnen, muss erstellt, gespeichert und analysiert werden.

4.2.2 Verfahren

[In diesem Verfahren geht es um die Protokollierung für alle Systeme und Netzwerke. Es wird erklärt, wie die Organisation Protokolle erfasst, speichert und schützt. Protokolle sind für die Reaktion auf Zwischenfälle (IR) von entscheidender Bedeutung, daher ist es auch wichtig zu erklären, wie sie im Falle einer IR verwendet werden. Ändern Sie diesen Abschnitt, sofern Sie ein anderes Verfahren in Ihrer Organisation praktizieren. Beachten Sie, dass ein Auditor nach dokumentierten Nachweisen für den beschriebenen Prozess verlangen wird. Seien Sie daher für ein Audit entsprechend vorbereitet und in der Lage, dokumentierte Nachweise für die Durchführung eines solchen Prozesses in einem Audit vorzuzeigen].

Anforderungen an die Protokollierung:

1. Bestimmen Sie den Zweck, für den Protokolle erstellt werden, und geben Sie die zu erfassenden und zu protokollierenden Daten sowie alle protokollspezifischen Anforderungen an.

2. Bestimmen Sie die Ereignisse, die protokolliert werden müssen, einschließlich erfolgreicher und abgewiesener Zugriffsversuche, Änderungen der Systemkonfiguration, Verwendung von Berechtigungen und Dateizugriffsaktivitäten.

3. Dokumentieren Sie die Details, die in jedem Protokollereignis enthalten sein sollen, z. B. Benutzer-IDs, Systemaktivitäten, Datum, Uhrzeit, Geräteidentität und Netzwerkadressen.

Erstellung und Sammlung von Protokollen:

1. Konfigurieren Sie Informationssysteme und Netzwerkgeräte so, dass sie Protokolle entsprechend den festgelegten Protokollierungsanforderungen erstellen.

2. Stellen Sie sicher, dass für alle relevanten Ereignisse, die in den Protokollierungsanforderungen festgelegt sind, Protokolle erstellt werden.

3. Implementieren Sie Mechanismen zum Sammeln von Protokollen von verschiedenen Systemen und Geräten in einem zentralen Protokollspeicher.

Log-Schutz:

1. Implementieren Sie Zugriffskontrollen, um den unbefugten Zugriff auf Protokolldaten zu verhindern, und stellen Sie sicher, dass nur autorisiertes Personal die Berechtigung hat, Protokolle einzusehen oder zu ändern.

2. Aktivieren Sie Mechanismen zum Schutz von Protokollen vor Manipulationen oder unbefugten Änderungen, wie z. B. kryptografisches Hashing, Nur-Anhang-Dateien oder Nur-Lese-Berechtigungen für Dateien.

3. Überprüfen Sie regelmäßig die Zugriffsprotokolle, um unbefugte Zugriffsversuche auf Protokolldaten zu erkennen und zu beseitigen.

Log-Analyse:

1. Erstellen Sie einen Zeitplan für die regelmäßige Analyse der Protokolle, um ungewöhnliche Aktivitäten oder anormales Verhalten zu erkennen.

2. Beauftragen Sie qualifiziertes Personal mit der Analyse von Protokollen unter Verwendung geeigneter Tools und Techniken, einschließlich vorgegebener Regeln, Verhaltensmuster, Trendanalysen und Bedrohungsdaten.

3. Dokumentieren Sie die Ergebnisse der Protokollanalyse, einschließlich aller festgestellten Sicherheitsvorfälle oder potenziellen Bedrohungen.

Reaktion auf Vorfälle:

1. Legen Sie eine angemessene Reaktion auf Sicherheitsvorfälle fest, die durch Warnungen aus der Protokollanalyse erkannt wurden, einschließlich Eskalationspfaden und Maßnahmen zur Risikominderung.

2. Verwenden Sie Protokolldaten als Beweismittel für die Untersuchung von Sicherheitsvorfällen, wobei die Integrität der Protokolldaten während des gesamten Untersuchungsprozesses zu gewährleisten ist.

Tools und Technologien zur Protokollverwaltung:

1. Setzen Sie geeignete Tools für die Protokollverwaltung ein, z. B. Dienstprogramme, Audit-Tools oder SIEM-Systeme, um die Protokollanalyse und -berichterstattung zu erleichtern.

2. Richten Sie eine entsprechende Konfiguration und Wartung von SIEM-Systemen gemäß Best Practices, einschließlich der Identifizierung geeigneter Protokollquellen, der Abstimmung von Regeln und der Entwicklung von Anwendungsfällen ein.

Überlegungen zur Cloud-Umgebung:

1. Alle Protokollierungsaktivitäten müssen gemäß den Empfehlungen und bewährten Verfahren des Cloud-Anbieters aktiviert werden.

2. Nutzen Sie bereitgestellte Analysedienste zur Überwachung und Optimierung des Cloud-Betriebs.[Beispiel: AWS CloudWatch Logs Insights und Azure Monitor Log Analytics]

3. Überprüfen Sie die Protokolle aller Cloud-Dienste in der Produktion.

4.3 Überwachungsaktivitäten

4.3.1 Richtlinie

Das Unternehmen muss Richtlinien für die Überwachung von Netzwerken, Systemen und Anwendungen aufstellen, um anomales Verhalten und potenzielle Informationssicherheitsvorfälle zu erkennen. Diese Richtlinie gilt für alle Mitarbeiter, Auftragnehmer und Drittnutzer, die Zugang zu den Netzen, Systemen und Anwendungen des Unternehmens haben. Sie umfasst die Überwachung des ein- und ausgehenden Netzwerkverkehrs, des Zugriffs auf Systeme und Anwendungen, der Systemkonfigurationen, der Protokolle der Sicherheitstools, der Ereignisprotokolle, der Ressourcennutzung und des Benutzerverhaltens.

4.3.2 Verfahren

[Dieses Verfahren ähnelt dem des Kapitels "4.2 - Protokollierung"; allerdings geht es hier viel mehr um die aktive Überwachung von Geräten (einschließlich ihrer Protokolle), als darum, wie Sie die Protokolle speichern und wie sie im Betrieb verwendet werden. Hierzu gehören Metriken und Daten wie das Nutzerverhalten und bestimmte Muster von Ereignissen aus der Vergangenheit].

Festlegung der Grundlinie:

1. Ermitteln Sie die wichtigen Leistungsindikatoren (KPIs) und Metriken, um eine Grundlage für das normale Verhalten von Netzwerken, Systemen und Anwendungen zu schaffen.

2. Sammeln Sie historische Daten über Netzwerkverkehr, Systemauslastung, Benutzerverhalten und Sicherheitsereignisse, um normale Muster zu analysieren und zu bestimmen.

3. Dokumentieren Sie die ermittelte Basislinie als Referenz für die Überwachungsaktivitäten.

Überwachung der Konfiguration:

1. Konfigurieren Sie Überwachungssysteme, um ein- und ausgehenden Netzwerkverkehr, Systemprotokolle, Ereignisprotokolle und Benutzeraktivitäten zu erfassen und zu analysieren.

2. Implementieren Sie Tools für die kontinuierliche Überwachung, die große Datenmengen verarbeiten und Warnmeldungen in Echtzeit liefern können.

3. Richten Sie die automatische Generierung von Warnmeldungen auf der Grundlage vordefinierter Schwellenwerte ein und stellen Sie sicher, dass das System so eingestellt ist, dass Fehlalarme minimiert werden.

4. Definieren Sie Eskalationsverfahren für Warnmeldungen, die sofortige Aufmerksamkeit erfordern, und gewährleisten Sie die Redundanz bei den Warnmeldemechanismen.

Erkennung von Anomalien:

1. Überwachen Sie den Netzwerkverkehr auf ungewöhnliche Muster, z. B. Spitzen im Datenübertragungsvolumen oder Verbindungen zu verdächtigen IP-Adressen.

2. Überwachen Sie System- und Anwendungsprotokolle auf unbefugte Zugriffsversuche, Änderungen an der Systemkonfiguration und abnormales Benutzerverhalten.

3. Analysieren Sie Leistungsmetriken, um Abweichungen von der normalen Ressourcennutzung festzustellen und mögliche Engpässe oder Überlastungen zu ermitteln.

4. Nutzen Sie spezielle Tools und Techniken zur Erkennung von Malware-Aktivitäten, einschließlich Intrusion Detection Systems (IDS) und Antivirus-Lösungen.

Behandlung und Reaktion auf Alarme:

1. Benennen Sie Mitarbeiter, die für die Überwachung von Warnmeldungen und die Untersuchung potenzieller Sicherheitsvorfälle zuständig sind.

2. Reagieren Sie umgehend auf Warnmeldungen, indem Sie die Art des Vorfalls überprüfen, seinen Schweregrad einschätzen und geeignete Verfahren zur Reaktion auf den Vorfall einleiten.

3. Dokumentieren Sie alle Maßnahmen, die während der Reaktion auf den Vorfall ergriffen wurden, einschließlich aller Abhilfemaßnahmen oder der Eskalation an höhere Stellen.

4. Kommunizieren Sie Ergebnisse und Empfehlungen an die relevanten Interessengruppen, einschließlich IT-Personal, Sicherheitsteams und Management.

Fehlalarm-Management:

1. Entwickeln Sie Verfahren zur Erkennung und Behebung von Fehlalarmen, die von Überwachungssystemen erzeugt werden.

2. Überprüfen und verfeinern Sie regelmäßig die Warnschwellenwerte und Erkennungsregeln, um Fehlalarme zu minimieren, ohne die Erkennungsfunktionen zu beeinträchtigen.

3. Dokumentieren Sie falsch-positive Vorfälle und analysieren Sie die Ursachen, um die Wirksamkeit der Überwachungsinstrumente und -prozesse zu verbessern.

Schulung und Sensibilisierung:

1. Schulen Sie das mit der Sicherheitsüberwachung betraute Personal in Bezug auf die Verwendung von Überwachungsinstrumenten, die Interpretation von Warnmeldungen und Verfahren zur Reaktion auf Zwischenfälle.

2. Führen Sie regelmäßig Sensibilisierungsveranstaltungen durch, um alle Mitarbeiter über die Bedeutung der Sicherheitsüberwachung und ihre Rolle bei der Meldung verdächtiger Aktivitäten zu unterrichten.

Dokumentation und Berichterstattung:

1. Führen Sie umfassende Aufzeichnungen über alle Überwachungsaktivitäten, einschließlich der Erstellung von Basisdaten, der Erkennung von Anomalien, der Behandlung von Warnungen und der Reaktion auf Vorfälle.

2. Erstellen Sie regelmäßige Berichte mit einer Zusammenfassung der Überwachungsergebnisse, einschließlich bemerkenswerter Ereignisse, Trends und Empfehlungen für Verbesserungen.

3. Bewahren Sie Überwachungsdaten in Übereinstimmung mit den Organisationsrichtlinien und den rechtlichen Anforderungen für Audits und forensische Analysen auf.

Überprüfung und kontinuierliche Verbesserung:

1. Überprüfen Sie regelmäßig die Überwachungsverfahren, -instrumente und -effektivität, um verbesserungswürdige Bereiche zu ermitteln.

2. Beziehen Sie Rückmeldungen aus Untersuchungen von Vorfällen, Sicherheitsbewertungen und Audits zur Verbesserung der Überwachungsmöglichkeiten und Reaktionsstrategien ein.

3. Aktualisieren Sie Überwachungsunterlagen und -verfahren bei Bedarf, um Änderungen in der Technologie, den Bedrohungen oder den organisatorischen Anforderungen Rechnung zu tragen.

4.4 Web-Filterung

4.4.1 Richtlinie

Die Filterung von Websites mit potenziell bösartigen Inhalten muss implementiert werden, um die Angreifbarkeit durch bösartige Inhalte zu verringern, Systeme vor Malware zu schützen und den Datenabfluss zu verhindern.

4.4.2 Verfahren

[Dieses Verfahren zeigt, wer die verantwortlichen Personen sind und welche Methoden in Ihrer Organisation zur Verwaltung der Webfilterung eingesetzt werden. Bei der Webfilterung geht es darum, den Datenverkehr zu reduzieren, indem der Zugang meist mit Hilfe von Tools herausgefiltert wird. Dies kann für Websites gelten, die nicht den Richtlinien der Organisation entsprechen, oder für Websites, die bekanntermaßen Malware enthalten. Ändern Sie diesen Abschnitt, sofern Sie ein anderes Verfahren in Ihrer Organisation praktizieren. Beachten Sie, dass ein Auditor nach dokumentierten Nachweisen für den beschriebenen Prozess verlangen wird. Seien Sie daher für ein Audit entsprechend vorbereitet und in der Lage, dokumentierte Nachweise für die Durchführung eines solchen Prozesses in einem Audit vorzuzeigen].

Rollen & Zuständigkeiten: [ändern Sie diese, wenn Sie andere Rollen oder Zuständigkeiten haben]

IT-Abteilung:

- Verantwortlich für die Einführung und Aufrechterhaltung von Maßnahmen zur Überprüfung und Filterung des Webzugriffs.
- Durchführung regelmäßiger Audits und Bewertungen, um die Einhaltung der Richtlinie zu gewährleisten.
- Bereitstellung von technischer Unterstützung und Hilfe bei der Implementierung der Web-Zugangskontrolle.

Abteilung Human Resources:

- Unterstützung bei der Entwicklung und Verbreitung von Schulungsmaterial im Zusammenhang mit der Web-Zugangskontrollrichtlinie.
- Unterstützung von Personalschulungsinitiativen zur sicheren und angemessenen Nutzung von Online-Ressourcen.

Verfahren:

Identifizierung der zu blockierenden Website-Kategorien:

- Arbeiten Sie mit den relevanten Interessengruppen zusammen, um die Arten von Websites zu ermitteln, die aufgrund von organisatorischen Anforderungen und Sicherheitsüberlegungen zu sperren sind.
- Erstellen Sie eine Liste bekannter oder vermuteter bösartiger Websites, Command-and-Control-Server und Websites mit illegalen Inhalten.

Festlegung von Regeln für den Webzugang:

- Entwickeln Sie Regeln für die sichere und angemessene Nutzung von Online-Ressourcen, einschließlich Beschränkungen für den Zugriff auf unerwünschte oder ungeeignete Websites und webbasierte Anwendungen.
- Dokumentieren Sie die Regeln und stellen Sie sicher, dass sie dem gesamten Personal wirksam vermittelt werden.

Konfiguration von Web-Filter-Tools:

- Konfigurieren Sie Webfilter-Tools, um den Zugriff auf bestimmte Kategorien von Websites zu blockieren, darunter solche mit Funktionen zum Hochladen von Informationen, bekannte bösartige Websites und Plattformen zum Austausch illegaler Inhalte.
- Stellen Sie sicher, dass die Web-Filter-Tools regelmäßig aktualisiert werden, um die neuesten Bedrohungsdaten zu berücksichtigen.

5 Kryptographische Verschlüsselung

5.1 Einsatz von Kryptographie

5.1.1 Richtlinie

Zum Schutz der Vertraulichkeit, Authentizität und Integrität von Informationen über sensible Daten müssen Kryptographie und eine sichere Schlüsselverwaltung eingesetzt werden.

5.1.2 Verfahren

[Es werden kryptografische Maßnahmen ergriffen, um sicherzustellen, dass die Verschlüsselung nach einem korrekten Standard erfolgt. Es wird Ihnen helfen zu verwalten, wer für die Überwachung der kryptografischen Maßnahmen verantwortlich ist und wer die Liste der Schlüssel führt. Ändern Sie diesen Abschnitt, sofern Sie ein anderes Verfahren in Ihrer Organisation praktizieren. Beachten Sie, dass ein Auditor nach dokumentierten Nachweisen für den beschriebenen Prozess verlangen wird. Seien Sie daher für ein Audit entsprechend vorbereitet und in der Lage, dokumentierte Nachweise für die Durchführung eines solchen Prozesses in einem Audit vorzuzeigen].

Rollen & Zuständigkeiten: [ändern Sie diese, wenn Sie andere Rollen oder Zuständigkeiten haben]

Abteilung IT-Sicherheit:

- Verantwortlich für die Beaufsichtigung der Umsetzung von Maßnahmen zur Nutzung von Kryptographie und Schlüsselverwaltung.
- Durchführung regelmäßiger Audits und Bewertungen, um die Einhaltung der Richtlinie zu gewährleisten.
- Bereitstellung von technischer Unterstützung und Hilfe bei kryptografischen Fragen.

Beauftragter für das Schüssel-Management:

- Die Organisation muss eine Person bennen, die für die Verwaltung kryptografischer Schlüssel und damit zusammenhängender Prozesse zuständig ist.
- Die Implementierung einer Schlüsselverwaltung, einschließlich der Erzeugung, Verteilung, Speicherung, Verwendung, Ersetzung und Vernichtung von kryptografischen Schlüsseln muss gewährleistet sein.

Verfahren:

Einhaltung der themenspezifischen Kryptographie-Richtlinie:

- Stellen Sie die Einhaltung der themenspezifischen Kryptographierichtlinien der Organisation, einschließlich der Grundsätze für den Informationsschutz sicher.
- Überprüfen Sie die in der Richtlinie beschriebenen Anforderungen und setzen diese um.

Identifizierung der kryptographischen Anforderungen:

- Bestimmen Sie die erforderlichen Schutzniveaus und die Klassifizierung von Informationen, um geeignete kryptografische Algorithmen auszuwählen.
- Identifizieren Sie Anwendungsfälle, in denen Kryptographie benötigt wird, um die Ziele der Informationssicherheit zu erreichen (z. B. Vertraulichkeit, Integrität, Authentifizierung).

Durchführung von Kryptographiemaßnahmen:

- Setzen Sie kryptografische Lösungen zum Schutz sensibler oder kritischer Informationen ein, unabhängig davon, ob diese gespeichert oder übertragen werden.
- Konfigurieren Sie Verschlüsselung, digitale Signaturen oder Nachrichtenauthentifizierungscodes auf der Grundlage der ermittelten Anforderungen.
- Stellen Sie die Einhaltung genehmigter kryptographischer Algorithmen, Verschlüsselungsstärken und Verwendungspraktiken fest.

Überwachung und Einhaltung:

- Führen Sie regelmäßige Audits von kryptografischen Implementierungen und Schlüsselverwaltungspraktiken durch, um die Einhaltung von Richtlinien und Standards zu gewährleisten.
- Überwachen Sie die Aktivitäten der Schlüsselverwaltung, einschließlich Schlüsselerzeugung, -verteilung und -verwendung, um Anomalien oder Sicherheitsvorfälle zu erkennen.

Dokumentation und Berichterstattung:

- Dokumentieren Sie die kryptografischen Maßnahmen, einschließlich Konfigurationen, Schlüsselverwaltungsverfahren und Prüfprotokolle.
- Erstellen Sie regelmäßige Berichte über die Verwendung von Kryptographie, die Schlüsselverwaltung und den Stand der Einhaltung der Vorschriften zur Überprüfung durch das Management.

6 Datenmaskierung

6.1 Datenmaskierung

6.1.1 Richtlinie

Datenmaskierungstechniken müssen eingesetzt werden, um die Offenlegung sensibler Daten, einschließlich personenbezogener Informationen, zu begrenzen.

6.1.2 Verfahren

[Das Datenmaskierungsverfahren stellt sicher, dass bei der Speicherung oder Übermittlung von Daten nur die erforderlichen Teile der Daten lesbar sind. Dies ist vergleichbar mit der Speicherung von Kreditkartendaten, die mit einem "*" anstelle der Zahlen auf den Quittungen gespeichert werden, die Sie in einem Geschäft erhalten. Hier wird gezeigt, wie man Daten maskiert, welche Daten man maskiert und wie man die zu maskierenden Daten identifiziert. Ändern Sie diesen Abschnitt, sofern Sie ein anderes Verfahren in Ihrer Organisation praktizieren. Beachten Sie, dass ein Auditor nach dokumentierten Nachweisen für den beschriebenen Prozess verlangen wird. Seien Sie daher für ein Audit entsprechend vorbereitet und in der Lage, dokumentierte Nachweise für die Durchführung eines solchen Prozesses in einem Audit vorzuzeigen].

Identifizierung von sensiblen Daten:

1. Dateneigentümer und relevante Stakeholder müssen sensible Daten in Systemen, Datenbanken und Anwendungen im Asset Management identifizieren und sie mit den entsprechenden Kennzeichnungen versehen.
2. Bestimmen Sie die Arten von sensiblen Daten, die aufgrund ihrer Sensibilität und der potenziellen Auswirkungen einer Offenlegung maskiert werden müssen.

Auswahl der Datenmaskierungstechniken:

1. Wählen Sie geeignete Datenmaskierungstechniken, wie Anonymisierung, Pseudonymisierung, Verschlüsselung oder Hashing, auf der Grundlage der ermittelten Anforderungen aus.
2. Stellen Sie sicher, dass die gewählten Techniken mit den rechtlichen, regulatorischen und vertraglichen Verpflichtungen übereinstimmen.

Implementierung der Datenmaskierung:

1. Wenden Sie Datenmaskierungstechniken nur gemäß den festgelegten Grundsätzen und Leitlinien an.
2. Verwenden Sie Tools und Technologien zur Maskierung sensibler Daten in Datenbanken, Dateien oder anderen Speichersystemen.

Prüfung und Validierung:

1. Führen Sie Tests durch, um sicherzustellen, dass Datenmaskierungstechniken effektiv angewandt werden und dass sensible Daten angemessen geschützt sind.
2. Validieren Sie den Maskierungsprozess, um sicherzustellen, dass die Originaldaten nicht rekonstruiert oder mit Hilfe der maskierten Daten neu identifiziert werden können.

7. Norm-Referenzen

7.1 Normreferenzen zu ISO27001:2022

Kapitel in diesem Dokument	Normkapitel (ISO27001:2022)
1. **Einleitung**	

2. **Systemkonfiguration und deren Schutz**	
• 2.1 Schutz vor Maleware	A 8.7
• 2.2 Handhabung von technischen Schwachstellen	A 8.8
• 2.3 Konfigurationsmanagement	A 8.9
• 2.4 Synchronisierung der Systemuhrzeit	A 8.17
• 2.5 Verwendung von Hilfsprogramme mit privilegierten Rechten	A 8.18
• 2.6 Installation von Software auf betrieblichen Systemen	A 8.19
3. **Netzwerke und Informationsübertragung**	
• 3.1 Informationsübertragung	A 5.14
• 3.2 Sicherheit der Netze	A 8.20
• 3.3 Sicherheit der Netzdienste	A 8.21
• 3.4 Trennung von Netzen	A 8.22
4. **Protokollierung, Überwachung und Web-Filterung**	
• 4.1 Verhinderung von Datenverlusten	A 8.12
• 4.2 Protokollierung	A 8.15
• 4.3 Überwachungsaktivitäten	A 8.16
• 4.4 Web-Filterung	A 8.23
5. **Kryptographische Verschlüsselung**	
• 5.1 Einsatz von Kryptographie	A 8.24
6. **Datenmaskierung**	
• 6.1 Datenmaskierung	A 8.11

7.2 Referenzen zu TISAX-ISA 6.0

Kapitel in diesem Dokument	Normkapitel (ISA-TISAX 6.0)
1. **Einleitung**	
2. **Systemkonfiguration und deren Schutz**	
• 2.1 Schutz vor Maleware	5.2.3
• 2.2 Handhabung von technischen Schwachstellen	5.2.5; 5.2.6
• 2.2 Konfigurationsmanagement	1.2.4; 4.1.3; 4.2.1; 5.2.3
• 2.3 ynchronisierung der Systemuhrzeit	5.2.5
• 2.4 Verwendung von Hilfsprogramme mit privilegierten Rechten	4.2.1
• 2.5 Installation von Software auf betrieblichen Systemen	5.2.5
3. **Netzwerke und Informationsübertragung**	
• 3.1 Informationsübertragung	5.1.2
• 3.2 Sicherheit der Netze	5.2.7
• 3.3 Sicherheit der Netzdienste	3.1.1; 5.3.2
• 3.4 Trennung von Netzen	5.2.7
4. **Protokollierung, Überwachung und Web-Filterung**	
• 4.1 Verhinderung von Datenverlusten	5.1.2
• 4.2 Protokollierung	5.2.4; 5.3.2
• 4.3 Überwachungsaktivitäten	5.2.4
• 4.4 Web-Filterung	1.3.3; 1.3.4
5. **Kryptographische Verschlüsselung**	
• 5.1 Einsatz von Kryptographie	5.1.1

6. **Datenmaskierung**	
• 6.1 Datenmaskierung	5.3.1