

1. Einleitung

Informationssicherheit sichert die strategischen und operativen Geschäftsprozesse der Berndorf Gruppe, die wesentlich auf Informations-, Kommunikations- und operativen Technologien (IT/OT) beruhen. Diese Richtlinie soll ein angemessenes, wirksames Sicherheitsniveau für Verfügbarkeit, Integrität und Vertraulichkeit von Informationen sowie IT- und OT-Systemen gewährleisten. Damit sollen Betriebsunterbrechungen, Datenverluste, finanzielle Schäden sowie Reputations- und Vertrauensverluste vermieden werden.

Sie legt einen einheitlichen, verbindlichen Mindeststandard für alle Gesellschaften fest. Grundlage sind die Richtlinie (EU) 2022/2555 (NIS-2) und die jeweils anwendbaren nationalen Umsetzungsgesetze in Österreich und Deutschland. Gesetzlich betroffene Gesellschaften müssen alle einschlägigen gesetzlichen und regulatorischen Anforderungen vollständig und fristgerecht erfüllen. Die Mindestanforderungen dieser Richtlinie gelten unabhängig von der gesetzlichen Betroffenheit für sämtliche Gesellschaften.

2. Geltungsbereich

Alle Gesellschaften der Berndorf Gruppe müssen diese Mindestanforderungen umsetzen. Ergänzende oder strengere eigene Richtlinien und Arbeitsanweisungen sind zulässig. Die Richtlinie gilt für:

- alle informationsverarbeitenden Systeme, Netzwerke, Anwendungen und Daten;
- alle IT- und OT-Systeme, insbesondere Produktions-, Steuerungs- und Automatisierungssysteme;
- alle Mitarbeiter sowie externe Dienstleister, Lieferanten, Auftragnehmer und sonstige Dritte mit Zugriff auf Systeme oder Daten der Gesellschaften.

Die Gesellschaften stellen die Einhaltung durch ihre Mitarbeiter sicher. Bei externen Partnern sind die je nach Leistung, Zugriff und Risiko relevanten Sicherheitsanforderungen vertraglich und organisatorisch abzusichern.

Die erstmalige Prüfung und Einstufung nach den nationalen NIS-2-Umsetzungsvorschriften erfolgte auf Konzernebene. Änderungen der Geschäftstätigkeit, Unternehmensgröße, Konzernstruktur oder technischen bzw. operativen Organisation, die diese Einstufung beeinflussen können, sind unverzüglich der zuständigen Stelle der Berndorf AG zu melden.

Die Einstufung ist mindestens jährlich und bei wesentlichen Veränderungen anlassbezogen mit der zuständigen Stelle der Berndorf AG zu überprüfen und nachvollziehbar zu dokumentieren.

3. Ziele der Informationssicherheit

3.1. Sicherheitsbewusstsein

Technische und organisatorische Maßnahmen wirken nur ausreichend, wenn alle Beschäftigten Risiken kennen und in ihrem Aufgabenbereich verantwortlich handeln. Risikomanagement nach Punkt 5.1 und regelmäßige Schulungen für Mitarbeiter und Management nach Punkt 5.3 sind daher unverzichtbar.

Konzern | Informationssicherheitsrichtlinie

3.2. Gesetzliche und vertragliche Pflichten

Die Maßnahmen dienen der Einhaltung aller relevanten gesetzlichen, regulatorischen und vertraglichen Anforderungen, insbesondere der NIS-2-Vorgaben.

3.3. Vermeidung materieller Schäden

Finanzielle Schäden durch Datenverlust, Manipulationen und Systemausfälle sollen verhindert werden.

3.4. Persönlichkeitsrechte und Betriebsgeheimnisse

Vertraulichkeit und Integrität personenbezogener Daten, Geschäftsgeheimnisse und aller weiteren wichtigen Unternehmensinformationen sind unabhängig von ihrer Form zu schützen. Für elektronische Dokumente und Informationen sind klare Geheimhaltungsanweisungen festzulegen und einzuhalten.

3.5. Schutz der Reputation

Die Richtlinie schafft eine Grundlage zur Vermeidung von Sicherheitsvorfällen und damit verbundenen Reputations- und Vertrauensverlusten.

3.6. Kontinuierliche Verbesserung

Die Berndorf AG verbessert Prozesse und Maßnahmen der Informationssicherheit fortlaufend in Zusammenarbeit mit den Gesellschaften.

4. Verantwortlichkeiten und Governance

Die dezentrale Organisation erfordert klare Zuständigkeiten auf Konzern- und Gesellschaftsebene.

4.1. Konzern / Berndorf AG

- Vorstand: trägt die nicht delegierbare Gesamtverantwortung, genehmigt die Richtlinie, lässt sich regelmäßig über Risiken, Vorfälle und Maßnahmen berichten und nimmt an Sicherheitsschulungen teil.
- Bee Security GmbH / Konzern-Informationssicherheitsbeauftragter: leitet und koordiniert die konzernweiten Aktivitäten, stellt Methoden und Vorlagen bereit, führt Risikoanalysen und jährliche konzernweite Security-Audits durch und berichtet darüber.
- IT-Abteilung: setzt technische Sicherheitsmaßnahmen um und sichert die Systemverfügbarkeit. Mitarbeiter halten die Sicherheitsrichtlinien ein und melden Vorfälle.

4.2. Teilkonzern / Tochtergesellschaft

- Geschäftsführung: verantwortet die Umsetzung der Richtlinie und der anwendbaren Gesetze, stellt Ressourcen bereit und lässt Abweichungen innerhalb angemessener Fristen beheben. Sie lässt sich regelmäßig über Risiken informieren, nimmt an Schulungen teil und meldet einstufigsrelevante Änderungen gemäß Punkt 2.
- Informationssicherheitsbeauftragter: leitet und koordiniert die lokalen Aktivitäten, koordiniert und dokumentiert Risikoanalysen, unterstützt Audits und verfolgt daraus abgeleitete Maßnahmen nach.

- IT-Abteilung: setzt technische Sicherheitsmaßnahmen um und sichert die Systemverfügbarkeit. Mitarbeiter halten die Sicherheitsrichtlinien ein und melden Vorfälle.

5. Verbindliche Mindestanforderungen

5.1. IT-Risikomanagement

Ein dokumentierter IT-Risikomanagement-Prozess ist verpflichtend. Aus der Analyse der Geschäftsprozesse und Risiken sind Kontrollen und Maßnahmen abzuleiten, die Schäden verhindern oder begrenzen. Vorlagen der Berndorf AG können zum Aufbau oder zur Überprüfung des Prozesses verwendet werden.

Der Prozess umfasst mindestens Business Impact Analyse (BIA) zur Ermittlung der Geschäftsprozesse und ihrer Kritikalität, Strukturanalyse, Schutzbedarfsanalyse, Risikobewertung, Risikobehandlung sowie regelmäßige Überprüfung und Aktualisierung mindestens jährlich oder anlassbezogen. Die Ergebnisse sind zu dokumentieren.

Die Dokumentation enthält mindestens betroffene Geschäftsprozesse und IT-/OT-Systeme, Kritikalität, verantwortliche Personen, identifizierte Risiken, bestehende und geplante Maßnahmen, Maßnahmenverantwortliche, Umsetzungsfristen und Restrisiken. Wesentliche Restrisiken sind der Geschäftsführung zur Entscheidung und dokumentierten Risikoakzeptanz vorzulegen. Der Prozess wird in den Security-Audits geprüft.

Die Geschäftsführung stellt die kurz-, mittel- und langfristig erforderlichen personellen, finanziellen und technischen Ressourcen für die Informationssicherheit sicher.

5.2. Zugriffskontrolle und Zugriffsrechte

Zugriffsrechte sind nach dem Prinzip der geringsten Rechte auf den erforderlichen Tätigkeitsumfang zu beschränken. Vergabe und wesentliche Änderungen administrativer oder sonstiger privilegierter Rechte benötigen eine dokumentierte Freigabe des zuständigen System-, Prozess- oder Datenverantwortlichen. Bei Eintritt, Aufgaben- oder Rollenwechsel und Austritt von Mitarbeitern oder externen Dienstleistern sind Rechte unverzüglich anzupassen oder zu entziehen.

Angemessene Authentifizierung ist verpflichtend. Multi-Faktor-Authentifizierung (MFA) ist insbesondere erforderlich für:

- administrative und sonstige privilegierte Zugriffe;
- Remote-Zugriffe von außerhalb des Unternehmensnetzwerks;
- administrative, privilegierte oder wartungsbezogene Zugriffe externer Dienstleister;
- Zugriffe auf cloudbasierte Administrationsoberflächen.

Technisch unmögliche MFA, insbesondere bei älteren OT-Systemen, ist zu dokumentieren und durch angemessene Maßnahmen wie Netzwerksegmentierung, abgesicherte Jump-Server, zeitlich begrenzte Freischaltungen oder verstärkte Protokollierung auszugleichen.

Privilegierte Berechtigungen und administrative, privilegierte oder wartungsbezogene externe Zugänge sind mindestens jährlich sowie anlassbezogen zu prüfen: fortbestehender Bedarf, eindeutige Identifizierbarkeit der Person bzw. des Dienstleisters, erforderlicher und angemessener Rechteumfang sowie Umsetzung der Schutzmaßnahmen, insbesondere MFA.

Konzern | Informationssicherheitsrichtlinie

Die jährliche Prüfung erfolgt im konzernweiten IT-Security-Audit. Gesellschaften liefern die nötigen Informationen und beheben Abweichungen fristgerecht. Eine separate jährliche Prüfung sämtlicher gewöhnlicher Benutzer-, Datei-, Ordner-, Laufwerks- oder SharePoint-Berechtigungen ist nicht erforderlich.

Ein aktuelles Verzeichnis privilegierter Personen und Konten sowie entsprechender externer Dienstleister ist zu führen. Es enthält mindestens Kontoinhaber bzw. Dienstleister, System, Art und Umfang der Rechte und die zuständige interne Stelle.

Administrative Rechte dürfen nicht geteilt werden. Personalisierte Administrationskonten sind von Benutzerkonten zu trennen, ausschließlich administrativ zu nutzen und gesondert abzusichern. Gemeinsam genutzte technische Konten sind nur zulässig, wenn personalisierte Konten technisch unmöglich oder aus nachvollziehbaren betrieblichen Gründen nicht zweckmäßig sind. Sie sind zu dokumentieren, besonders zu schützen und soweit technisch möglich nachvollziehbar zu protokollieren.

5.3. Informationssicherheitsbewusstsein und Schulung

Regelmäßige Sicherheitsschulungen sind verpflichtend. Jede Gesellschaft legt Zielgruppen und Umfang unter Berücksichtigung der Arbeitsbedingungen und Risiken fest. Mindestintervalle:

- Mitarbeiter: jährlich und beim Onboarding;
- Management: jährlich sowie anlassbezogen.

Konzern Legal, Bee Security GmbH oder andere qualifizierte interne bzw. externe Anbieter können die Schulungen durchführen. Konzern Legal und Bee Security GmbH können Unterlagen, organisatorische Unterstützung und personelle Kapazitäten bereitstellen.

Geeignete externe Schulungen sind zulässig; eigene Unterlagen oder interne Durchführung sind nicht erforderlich, wenn die relevanten Inhalte angemessen abgedeckt werden. Die Gesellschaft bleibt für die fristgerechte Durchführung verantwortlich. Inhalte, Durchführung und Teilnahme sind nachvollziehbar zu dokumentieren; bei externen Schulungen sind geeignete Nachweise aufzubewahren.

5.4. Physische und umweltbezogene Sicherheit

Fremde Personen dürfen nicht unbeaufsichtigt in Unternehmensräume gelangen. Zutrittskontrollen und organisatorische Maßnahmen müssen unbefugten Zugang zu sicherheitskritischen Bereichen verhindern, insbesondere Serverräumen, Netzwerkverteilern, Leitständen und Räumen mit kritischen IT-/OT-Komponenten.

Kritische IT-/OT-Systeme sind risikogerecht vor Feuer, Wasser, Stromausfällen, Überhitzung und weiteren relevanten Umweltgefahren zu schützen. Maßnahmen sind regelmäßig zu überprüfen und zu dokumentieren.

5.5. Sicherheit der Lieferkette

Ein dokumentierter, risikobasierter Prozess zur Ermittlung, Bewertung und Behandlung von Cyberrisiken in der Lieferkette ist einzurichten und aufrechtzuerhalten.

Konzern | Informationssicherheitsrichtlinie

Ermittlung relevanter Lieferanten

Unmittelbare Lieferanten, Dienstleister und sonstige Vertragspartner sind zunächst darauf zu prüfen, ob ihre Produkte, Dienste, Zugriffsrechte, digitalen Schnittstellen oder sonstige Einbindung die Sicherheit oder Verfügbarkeit der Netz- und Informationssysteme relevant beeinflussen können.

Gleichartige Lieferanten oder Gruppen können gemeinsam erstbeurteilt werden. Eine individuelle vertiefte Cyberrisikobewertung aller Lieferanten ist nicht erforderlich. Von weiteren Bewertungen können insbesondere Lieferanten ausgenommen werden, die sämtliche folgenden Voraussetzungen erfüllen:

- keine Bereitstellung von IKT-Produkten, -Diensten oder -Prozessen;
- kein Zugriff auf Systeme, Netzwerke oder schutzbedürftige Informationen;
- keine digitale Schnittstelle oder sonstige technische Anbindung;
- kein relevanter Einfluss eines Ausfalls oder einer Beeinträchtigung auf Sicherheit oder Verfügbarkeit der Netz- und Informationssysteme oder wesentlicher Geschäftsprozesse.

Erstbeurteilung und daraus abgeleitete Ausnahmen sind nachvollziehbar zu dokumentieren.

5.5. Sicherheit der Lieferkette (Fortsetzung)

Lieferantenverzeichnis

Für cyberrelevante unmittelbare Lieferanten, Dienstleister und Vertragspartner ist ein aktuelles Verzeichnis mit mindestens folgenden Angaben zu führen:

- Name sowie bezogene Produkte, Dienste oder Prozesse;
- zuständige interne Stelle bzw. verantwortlicher Fachbereich;
- betroffene Geschäftsprozesse und IT-/OT-Systeme;
- Art und Umfang von System-, Daten-, Remote- oder Administrationszugriffen;
- Risikoklassifikation, Datum und Ergebnis der letzten Bewertung;
- offene Maßnahmen und nächster Überprüfungstermin.

Risikoklassifikation

Cyberrelevante Lieferanten sind vor Beauftragung und danach risikobasiert als kritisch, hoch oder normal einzustufen. Bei bestehenden Lieferanten ist dies entsprechend ihrer Risikorelevanz nachzuholen. Der für Beschaffung oder Nutzung zuständige Fachbereich klassifiziert in Abstimmung mit IT oder Informationssicherheitsbeauftragtem und dokumentiert die Einstufung.

Zu berücksichtigen sind insbesondere:

- Zugriffsebene: Art und Umfang des Zugriffs auf Systeme, Netzwerke, OT-Systeme, Daten und Informationen;
- Abhängigkeit: Bedeutung für wesentliche Geschäftsprozesse und IT-/OT-Systeme sowie Ersetzbarkeit;
- Reife: Qualität und Wirksamkeit der Sicherheitsmaßnahmen;
- Vertrauen: Verlässlichkeit, Aktualität und Aussagekraft der Informationen und Nachweise;
- Auswirkungen von Ausfällen oder Sicherheitsvorfällen sowie Art und Schutzbedarf verarbeiteter Informationen;

Konzern | Informationssicherheitsrichtlinie

- administrative, privilegierte, wartungsbezogene und sonstige Remote-Zugriffe;
- sicherheitsrelevante Unterauftragnehmer sowie Sicherheit der Entwicklungs-, Wartungs- und Aktualisierungsprozesse.

Insbesondere Lieferanten, die kritische IT-/OT-Systeme betreiben oder wesentlich unterstützen, administrative bzw. privilegierte Rechte besitzen oder erhebliche Betriebsstörungen verursachen können, sind als kritisch einzustufen.

Bewertung der Cyberresilienz

Art und Umfang der Bewertung richten sich nach der Risikoklassifikation. Zur Beurteilung der Gesamtqualität und Cyberresilienz von Produkten und Diensten können insbesondere dienen:

- eigene dokumentierte Risikobewertungen und Selbstauskünfte;
- Bewertungen nach dem aktuellen Cyber Risk Rating Schema des Kompetenzzentrums Sicheres Österreich und des KSV1870;
- gültige Cyber Risk Ratings, Cyber Trust Labels und einschlägige Zertifizierungen;
- Audit-, Prüf- und Kontrollberichte, eigene Lieferantenaudits oder Audits qualifizierter Dritter sowie gleichwertige Nachweise.

Ein formelles Rating oder eine bestimmte Zertifizierung ist nicht generell verpflichtend, wenn andere geeignete, nachvollziehbar dokumentierte Maßnahmen eine angemessene Beurteilung erlauben. Zertifikate, Ratings und Auditberichte müssen die konkret bezogenen Produkte und Dienste abdecken, aktuell und ausreichend aussagekräftig sein.

5.5. Sicherheit der Lieferkette (Fortsetzung)

Sicherheitsanforderungen an Lieferanten

Für kritische Lieferanten sind, soweit für die Leistung relevant, insbesondere folgende erhöhte Anforderungen festzulegen:

- Nachweise eines angemessenen Informationssicherheitsniveaus;
- vertragliche Vorfallmeldepflichten, die eigene gesetzliche Meldungen rechtzeitig ermöglichen;
- Unterstützung bei Untersuchung, Eindämmung und Behebung von Vorfällen;
- Regeln für Unterauftragnehmer und die Weitergabe anwendbarer Sicherheitsanforderungen;
- Audit-, Kontroll-, Auskunfts- und Einsichtsrechte oder gleichwertige Nachweise;
- definierte Reaktions-, Notfall-, Wiederherstellungs- und Betriebskontinuitätsprozesse;
- angemessene Verfügbarkeits-, Wiederherstellungs- und Service-Level-Anforderungen;
- angemessene Haftungsregeln für Sicherheitsvorfälle und Vertragsverletzungen.

Bei hohem Risiko sind die leistungsbezogenen erforderlichen Anforderungen dieses Katalogs risikobasiert anzuwenden. Bei normalem Risiko können allgemeine Sicherheits- und Vertraulichkeitsanforderungen genügen.

Vertragliche Absicherung

Die Anforderungen sind vertraglich abzusichern. Je nach Art und Risiko der Leistung sind insbesondere zu berücksichtigen:

- Auftragsverarbeitungsvereinbarungen, soweit anwendbar, Geheimhaltungsvereinbarungen und Service Level Agreements;

Konzern | Informationssicherheitsrichtlinie

- sicherer Fernzugriff, insbesondere MFA, Protokollierung und Rechtevergabe;
- Melde- und Unterstützungspflichten bei Sicherheitsvorfällen;
- Unterauftragnehmer und Weitervergaben;
- Bereitstellung und Aktualisierung von Sicherheitsnachweisen;
- Datenlokalität und Datenverarbeitung gemäß anwendbaren gesetzlichen Vorgaben;
- sichere Entwicklungs-, Wartungs- und Aktualisierungsprozesse;
- bei sicherheitsrelevanter Software angemessene Transparenz über Dritt- und Open-Source-Komponenten;
- Beendigung der Leistung, insbesondere Datenrückgabe oder -löschung und Entzug der Zugriffsrechte.

Die Sicherheitsanforderungen gelten gleichermaßen für intern und extern betriebene Systeme und Dienste.

5.5. Sicherheit der Lieferkette (Fortsetzung)

Überprüfung und Monitoring

Lieferantenverzeichnis und Risikoklassifikation sind mindestens jährlich sowie bei wesentlichen Änderungen an Leistung, Zugriffsrechten, Unterauftragnehmern oder Risikosituation anlassbezogen zu prüfen und zu dokumentieren.

Die Cyberresilienz kritischer Lieferanten ist mindestens jährlich zu überprüfen. Bei übrigen cyberrelevanten Lieferanten bestimmen Risikoklassifikation und Risiko den Umfang und die Häufigkeit. Ohne wesentliche Änderungen können die Bestätigung bisheriger Angaben und die Prüfung relevanter Änderungen genügen.

Neubewertungen sind insbesondere bei erheblichen Sicherheitsvorfällen, wesentlichen Leistungsänderungen, neuen administrativen oder Remote-Zugängen, Ablauf oder Entzug von Sicherheitsnachweisen sowie begründeten Zweifeln an bisherigen Bewertungen erforderlich.

Risiken und Abweichungen sind mit geeigneten Maßnahmen zu behandeln; deren Umsetzung ist zu überwachen. Wesentliche Restrisiken sind der Geschäftsführung zur dokumentierten Entscheidung vorzulegen.

Die Prozessgestaltung, insbesondere Erstbeurteilung, Klassifikation, Bewertung und Nachweise, kann sich am aktuellen Cyber Risk Rating Schema des Kompetenzzentrums Sicheres Österreich und des KSV1870 (Anhang 1) orientieren. Abweichende Prozesse sind zulässig.

5.6. Betriebssicherheit und technischer Systembetrieb

Für den sicheren IT-/OT-Betrieb sind geeignete technische und organisatorische Maßnahmen umzusetzen, insbesondere Patch- und Vulnerability-Management, sichere Konfigurationen, zeitgemäße kryptografische Verfahren, abgesicherte Fernzugriffe und regelmäßige Wartung sicherheitskritischer Komponenten.

Konkrete Maßnahmen sind in technischen Richtlinien und Betriebsdokumentationen festzulegen. Maßgeblich sind einschlägige technische Kontrollen anerkannter Informationssicherheitsstandards und der Stand der Technik; eine bestimmte Zertifizierung ist nicht vorausgesetzt.

5.7. Notfallvorsorge und Wiederherstellung

Dieser Abschnitt regelt strategisches Notfall-, Wiederherstellungs- und Krisenmanagement zur Geschäftskontinuität; operative Vorfallobehandlung regelt Kapitel 6. Die Gesellschaften müssen umsetzen:

- Notfall- und Wiederherstellungsplanung: Pläne für kritische IT-/OT-Systeme, regelmäßige Datensicherungen sowie regelmäßige Prüfung und Validierung der Wiederherstellungsprozesse. Wiederherstellungsfähigkeit ist mindestens jährlich durch dokumentierten Wiederherstellungstest oder gleichwertige technische Validierung zu prüfen.
- Betriebskontinuität: Wiederanlaufziele, etwa RTO, RPO oder gleichwertige Parameter, festlegen und regelmäßig durch Tests und Reviews validieren.
- Notfallhandbuch und Übungen: Handbuch führen, regelmäßig strategische Notfall- und Krisenübungen durchführen, Ergebnisse dokumentieren und Verbesserungen ableiten.
- Krisenmanagement: Organisation, Rollen, Verantwortlichkeiten sowie Alarmierungs- und Kommunikationspläne festlegen; erforderlichenfalls mit internen und externen Stellen wie CERT, Behörden, Providern und Systemintegratoren abstimmen.

5.8. Sicherheit im Personalwesen

Geeignete Prozesse und Richtlinien müssen Integrität und Sicherheit des Personals gewährleisten. Erforderlich sind:

- Prüfung von Qualifikation und Vertrauenswürdigkeit neuer Mitarbeiter, beispielsweise durch Strafregistrauszug;
- geregelte Onboarding-, Change- und Offboarding-Prozesse;
- unverzügliche Anpassung von Zugriffs- und Zutrittsrechten bei Aufgaben- oder Rollenwechsel;
- Entzug dieser Rechte spätestens mit Wirksamwerden des Austritts;
- verbindliche Sicherheits- und IT-Richtlinien einschließlich Sanktionen bei Verstößen.

5.9. Sicherheitsarchitektur

Sichere Konfiguration und Härtung: Systeme und Anwendungen sind nach dokumentierten Härtungs- und Konfigurationsstandards abzusichern. Konfigurationsunterlagen sind aktuell zu halten; unnötige Dienste und Komponenten sind zu deaktivieren oder zu entfernen.

Asset- und Verantwortlichkeitsmodell: Für IT-/OT-Systeme, Komponenten, Softwareplattformen und Anwendungen ist ein aktuelles Inventar mit Kritikalitätsklassifikation und benannten Verantwortlichen (Owner) zu führen.

Netzwerksegmentierung und Schnittstellen: Netze sind entsprechend dem Schutzbedarf physisch oder logisch zu segmentieren. Segmentverbindungen sind auf das notwendige Minimum zu begrenzen. Drittschnittstellen zu Lieferanten oder Kunden, etwa Fernzugriff, Monitoring und Datenaustausch, sind abzusichern und zu dokumentieren.

Netzwerksicherheit: Eingehender, ausgehender und interner Verkehr ist zu filtern und auf das notwendige Maß zu reduzieren. Filterregeln sind regelmäßig zu prüfen und anzupassen.

5.10. Nutzung künstlicher Intelligenz (KI)

KI-Systeme sind gemäß den konzernweiten Vorgaben der Konzern-KI-Richtlinie zu nutzen. Bei möglichen sicherheits-, datenschutz- oder geschäftskritischen Auswirkungen müssen Gesellschaften ergänzende interne Regeln erstellen. Zu berücksichtigen sind insbesondere:

- Schutz vertraulicher Unternehmensinformationen;
- Datenübermittlungen an externe Systeme;
- Transparenz der Nutzung;
- Risikobewertung vor dem produktiven Einsatz.

6. Informationssicherheitsvorfälle

Jede Gesellschaft richtet einen dokumentierten Prozess zur Erkennung, Meldung, Bewertung und Behandlung von Sicherheitsvorfällen ein. Er regelt insbesondere die Erkennung sicherheitsrelevanter Ereignisse, die Folgenbewertung, operative Eindämmung und Wiederherstellung sowie interne und externe Meldepflichten.

Mitarbeiter und externe Personen müssen tatsächliche oder vermutete Vorfälle unverzüglich über den festgelegten internen Meldeweg an den Informationssicherheitsbeauftragten oder die interne Meldestelle melden. Eine abschließende Beurteilung durch die meldende Person ist nicht erforderlich.

a. Meldepflichten

Die benannte verantwortliche Stelle beurteilt gemeinsam mit Geschäftsführung und zuständigen Informationssicherheitsfunktionen, ob eine gesetzliche externe Meldepflicht besteht. Für Gesellschaften im Anwendungsbereich nationaler NIS-2-Umsetzungsvorschriften gelten die gesetzlichen Fristen:

- Frühwarnmeldung unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis;
- Detailmeldung innerhalb von 72 Stunden;
- Abschlussbericht nach Behebung des Vorfalls.

Zuständige nationale Meldestellen sind entsprechend den anwendbaren gesetzlichen Vorgaben einzubinden.

b. Eskalation und Abstimmung

Ablauf, Eskalationsstufen und Zuständigkeiten sind zwischen Incident Response sowie Notfall- und Krisenmanagement abzustimmen und verbindlich zu dokumentieren.

c. Tests und operative Übungen

Incident-Response-Prozesse sind regelmäßig zu testen, etwa durch Tabletop-Übungen oder technische Tests, und zu aktualisieren.

d. Forensische Fähigkeit

Forensisches Know-how und Kapazitäten sind intern vorzuhalten oder über vertraglich gesicherte Dienstleister verfügbar zu machen.

e. Lessons Learned

Erkenntnisse aus Vorfällen und Übungen sind zu dokumentieren und für die kontinuierliche Verbesserung zu nutzen.

7. Überwachung und Wirksamkeitsbewertung

Die Gesellschaften schaffen Prozesse zur laufenden Überwachung und Bewertung der Informationssicherheit. Geeignete Kennzahlen, Reifegradbewertungen oder Maßnahmen-Reviews sind in der IT-Richtlinie festzulegen. Umfang und Technik richten sich nach Systemkritikalität, Risikosituation und technischen Gegebenheiten. Eigene Systeme, zentrale Konzernlösungen oder geeignete externe Dienstleister sind zulässig.

7.1. Protokollierung und Monitoring

Kritische IT-/OT-Systeme, Sicherheitskomponenten, administrative Arbeitsstationen und zentrale Dienste sind zu protokollieren und zu überwachen. Logs sind mit Datum und Uhrzeit aus synchronisierten Zeitquellen zu erfassen, zentral zu speichern und für eine definierte Frist gesichert aufzubewahren. Aufbewahrungsfrist sowie Zuständigkeiten für Betrieb, Auswertung und Schutz der Protokollierungssysteme sind festzulegen und zu dokumentieren.

7.2. Korrelation und Analyse

Sicherheitsereignisse sind mit geeigneten Mechanismen, etwa zentraler Korrelation und Analyse, auszuwerten, um Vorfälle zeitnah zu erkennen und zu bewerten. Die Vertraulichkeit gespeicherter Protokolldaten ist sicherzustellen.

8. Dokumentation und Berichterstattung

Alle sicherheitsrelevanten Prozesse, Maßnahmen und Vorfälle sind nachvollziehbar zu dokumentieren. Die Dokumentation umfasst mindestens:

- Risikoanalysen sowie Verzeichnisse kritischer IT-/OT-Systeme und administrativer Zugänge;
- Lieferantenklassifikationen und Schulungsnachweise;
- Ergebnisse von Wiederherstellungs- und Notfalltests;
- Informationssicherheitsvorfälle und Auditfeststellungen;
- Umsetzungsstand der daraus abgeleiteten Maßnahmen.

Mindestens jährlich sowie bei wesentlichen Risiken, Vorfällen oder erheblichen Umsetzungsverzögerungen ist an die Geschäftsführung der obersten Gesellschaft des jeweiligen Teilkonzerns zu berichten. Diese berichtet über den aktuellen Stand im Teilkonzern an die Vorstände der Berndorf AG.

9. Jährliche Audits

Bee Security GmbH prüft Umsetzung und Einhaltung dieser Mindestanforderungen als zusätzlichen Prüfungspunkt der jährlichen konzernweiten Security-Audits. Für alle Teilkonzerne gilt ein einheitlicher Prüfungsansatz.

Abweichungen und Verbesserungspotenziale sind im Auditbericht festzuhalten. Für Abweichungen sind angemessene Maßnahmen, Verantwortliche und Fristen festzulegen; die Umsetzung ist nachzuverfolgen.

Konzern | Informationssicherheitsrichtlinie

Wesentliche Abweichungen oder Verzögerungen sind der Geschäftsführung der betroffenen Gesellschaft sowie im konzernweiten Berichtswesen den zuständigen Stellen der Berndorf AG zu melden.

10. Schlussbestimmungen

Die Informationssicherheitsrichtlinie tritt mit ihrer Veröffentlichung in Kraft. Sie ist regelmäßig zu überprüfen und bei Bedarf an aktuelle Anforderungen und Bedrohungslagen anzupassen.

Im Auftrag der Geschäftsführung:

Josef Unterberger