Anforderungen an die Cyber-Security zur Versicherbarkeit von Unternehmen

Vorbemerkung

Im Folgenden werden die technisch-organisatorischen Anforderungen zur Cyber-Security aufgeführt, wie wir sie von unseren Kunden erwarten. Sie können je nach Risiko bzw. Schutzbedarf im Einzelfall in unterschiedlichem Maße Anwendung finden. Es gilt dabei der Grundsatz der Angemessenheit. In jedem Fall sind gesetzliche Anforderungen (z. B. aus dem Datenschutzgesetz oder dem IT-Sicherheitsgesetz) sowie behördliche Auflagen zu berücksichtigen. Verbindlich für den Versicherungsnehmer sind stets ausschließlich die Regelungen im Versicherungsschein und in den jeweiligen Versicherungsbedingungen (z. B. Auflagen und Vorbehalte).

Die Kriterien unterliegen einer ständigen Weiterentwicklung und Anpassung an die Risikosituation sowie dem Stand der Technik.

Die einzelnen Anforderungen können in einer Art **Präventionskette** eingeordnet werden:

Nr.	Was?	Stichworte (beispielhaft)
1	Schwachstellen von außen erkennen	Schwachstellen-/Port-Scan – Penetrations-Tests
2	Mensch / User	Awareness – Phishing-Simulationen – Email-Security - MDM
3	Software-Schwachstellen	Asset-Management - Patchmanagement - kritische Patche - EoL-Systeme
4	Lateral Movement	Segmentierung - Netzwerküberwachung
5	Berechtigungen	Berechtigungsmanagement - Privilegierte Accounts – Fernzugriffe - MFA
6	Detektion und Reaktion	AV/EDR - NAC - IDS/IPS - Logfiles - SIEM/SOC
7	Backups	Backupkonzept - Schutz vor Manipulation - Restore-Tests
8	Vorbereitet sein	Notfallplan - Desaster Recovery – Übungen - BCM
9	Ständige Verbesserung	ISMS - Risikomanagement - Due Dilligence

Anforderungen an die Cyber-Security zur Versicherbarkeit von Unternehmen

Für Unternehmen bis 10 Mio. EUR wird auf das Antragsformular und die Obliegenheiten in den Bedingungen ByteProtect 5.1 Kompakt verwiesen. Auf eine Darstellung wird hier daher verzichtet. Die Zuordnung zur jeweilige Risikoklasse erfolgt final nach Prüfung individuell durch den Underwriter.

Die Farben neben den Anforderungen bedeuten:

Grün = Empfehlung gelb = Versicherungsschutz mit Auflage rot = Voraussetzung für den Versicherungsschutz

			Risikoklassen			
		Risikoklasse	**A**	**B**	**C**	**D**
		Umsatzbereich	10 bis 50 Mio. EUR	bis 250 Mio. EUR	bis 600 Mio. EUR	> 600 Mio. EUR
		Beschreibung	Geringe Komplexität, keine kritischen Branchen	Mittlere Komplexität, weniger kritische Branchen	Hohe Komplexität, kritische Branchen	Hochrisiko
		Risikoerfassung	Fragebogen	Fragebogen	Fragebogen + ggf. Risikogespräch	Fragebogen + Risikogespräch
	Anforderungskatalog					
Nr.	**Kriterium**	**Stichwort**		**Anforderung**	**Anforderung**	**Anforderung**
1	**Schwachstellen von außen erkennen**	Scans		Das Unternehmen führt mindestens jährlich Scans von außen auf die Webseite bzw. das eigene Netzwerk durch, um kritische offene Ports und mögliche Schwachstellen (vor allem veraltete Systeme) zu erkennen.	Das Unternehmen führt mindestens jährlich Scans von außen auf die Webseite bzw. das eigene Netzwerk durch, um kritische offene Ports und mögliche Schwachstellen (vor allem veraltete Systeme) zu erkennen.	Das Unternehmen führt mindestens jährlich Scans von außen auf die Webseite bzw. das eigene Netzwerk durch, um kritische offene Ports und mögliche Schwachstellen (vor allem veraltete Systeme) zu erkennen.
2	**Schwachstellen von außen erkennen**	Penetrations-Tests			Das Unternehmen führt mindestens alle zwei Jahre sowie bei neuen Web-Anwendungen Penetrations-Tests mit Hilfe von spezialisierten Dienstleistern durch, um mögliche Schwachstellen zu erkennen.	Das Unternehmen führt mindestens alle zwei Jahre sowie bei neuen Web-Anwendungen Penetrations-Tests mit Hilfe von spezialisierten Dienstleistern durch, um mögliche Schwachstellen zu erkennen.
3	**Awareness**	Grundsatz	Das Unternehmen führt für seine Mitarbeiter, die Zugang zu IT und Internet haben, mindestens jährlich Maßnahmen zur Förderung eines sicheren Umgangs mit Internet, IT und Daten durch.	Das Unternehmen führt für seine Mitarbeiter, die Zugang zu IT und Internet haben, mindestens jährlich Maßnahmen zur Förderung eines sicheren Umgangs mit Internet, IT und Daten durch.	Das Unternehmen führt für seine Mitarbeiter, die Zugang zu IT und Internet haben, mindestens jährlich Maßnahmen zur Förderung eines sicheren Umgangs mit Internet, IT und Daten durch.	Das Unternehmen führt für seine Mitarbeiter, die Zugang zu IT und Internet haben, mindestens jährlich Maßnahmen zur Förderung eines sicheren Umgangs mit Internet, IT und Daten durch.
4	**Awareness**	Schulungen			Diese Schulungen werden verpflichtend z. B. über Web-based Trainings angeboten. Die Durchführung wird nachgehalten und der Lernfortschritt dokumentiert.	Diese Schulungen werden verpflichtend z. B. über Web-based Trainings angeboten. Die Durchführung wird nachgehalten und der Lernfortschritt dokumentiert.
5	**Awareness**	Phishing			Es werden zusätzlich Phishing-Simulationen mindestens alle zwei Jahre durchgeführt.	Es werden zusätzlich Phishing-Simulationen mindestens alle zwei Jahre durchgeführt.
6	**Email-Security**	Grundsatz	Eingehende Emails werden hinsichtlich möglicher schädlicher Anhänge oder Internetlinks vor der Zustellung überprüft.	Eingehende Emails werden hinsichtlich möglicher schädlicher Anhänge oder Internetlinks vor der Zustellung überprüft.	Eingehende Emails werden hinsichtlich möglicher schädlicher Anhänge oder Internetlinks vor der Zustellung überprüft.	Eingehende Emails werden hinsichtlich möglicher schädlicher Anhänge oder Internetlinks vor der Zustellung überprüft.
7	**Email-Security**	Kennzeichnung "extern"		Emails, die von außerhalb des Unternehmens zugestellt werden, werden für den Empfänger deutlich als "extern" gekennzeichnet.	Emails, die von außerhalb des Unternehmens zugestellt werden, werden für den Empfänger deutlich als "extern" gekennzeichnet.	Emails, die von außerhalb des Unternehmens zugestellt werden, werden für den Empfänger deutlich als "extern" gekennzeichnet.
8	**Email-Security**	Aktive Inhalte		Dateien mit aktiven Inhalten und Makros von außerhalb des Unternehmens werden standardmäßig geblockt	Dateien mit aktiven Inhalten und Makros von außerhalb des Unternehmens werden standardmäßig geblockt	Dateien mit aktiven Inhalten und Makros von außerhalb des Unternehmens werden standardmäßig geblockt
9	**Email-Security**	SPF (Sender Policy Framework)		Das SPF zum Schutz vor gefälschten E-Mails wird angewendet und ist wirksam.	Das SPF zum Schutz vor gefälschten E-Mails wird angewendet und ist wirksam.	Das SPF zum Schutz vor gefälschten E-Mails wird angewendet und ist wirksam.

Nr.	Anforderungskatalog Kriterium	Stichwort			Anforderung		Anforderung		Anforderung	
10	**Patchmanagement**	Asset-Management	Das Unternehmen verfügt über eine Übersicht aller eingesetzter Soft- und Hardware.		Das Unternehmen verfügt über eine Übersicht seiner Soft- und Hardware, deren Patch-Stand, Funktion für das Unternehmen und deren jeweiliger Kritikalität.		Das Unternehmen verfügt über eine Übersicht seiner Soft- und Hardware, deren Patch-Stand, Funktion für das Unternehmen und deren jeweiliger Kritikalität.		Das Unternehmen verfügt über eine Übersicht seiner Soft- und Hardware, deren Patch-Stand, Funktion für das Unternehmen und deren jeweiliger Kritikalität.	
11	**Patchmanagement**	Netzwerk-Scanner			Mit Hilfe von Software-Tools werden interne Netzwerke hinsichtlich installierter Hard- und Software und deren Patch-Stand regelmäßig überprüft und überwacht (Netzwerk-Scanner). Dabei werden mind. 85 % der gesamten Infrastruktur des Unternehmens erfasst.		Mit Hilfe von Software-Tools werden interne Netzwerke hinsichtlich installierter Hard- und Software und deren Patch-Stand regelmäßig überprüft und überwacht (Netzwerk-Scanner). Dabei werden mind. 85 % der gesamten Infrastruktur des Unternehmens erfasst.		Mit Hilfe von Software-Tools werden interne Netzwerke hinsichtlich installierter Hard- und Software und deren Patch-Stand regelmäßig überprüft und überwacht (Netzwerk-Scanner). Dabei werden mind. 90 % der gesamten Infrastruktur des Unternehmens erfasst.	
12	**Patchmanagement**	Network-Access-Control (NAC)					Es ist ein Network-Access-Control (NAC) in Netzwerkbereichen installiert, in denen Dritte potentiell fremde Geräte anschließen können.		Es ist ein Network-Access-Control (NAC) in Netzwerkbereichen installiert, in denen Dritte potentiell fremde Geräte anschließen können.	
13	**Patchmanagement**	Updates	Das Unternehmen informiert sich regelmäßig über verfügbare Updates.		Das Unternehmen informiert sich regelmäßig über verfügbare Updates.		Das Unternehmen informiert sich regelmäßig über verfügbare Updates.		Das Unternehmen informiert sich regelmäßig über verfügbare Updates.	
14	**Patchmanagement**	Notfall-Patche			Es besteht ein Verfahren für das Aufspielen von Notfall-Patche bei besonders kritischen Schwachstellen.		Es besteht ein Verfahren für das Aufspielen von Notfall-Patche bei besonders kritischen Schwachstellen.		Es besteht ein Verfahren für das Aufspielen von Notfall-Patche bei besonders kritischen Schwachstellen.	
15	**Patchmanagement**	Kritische Schwachstellen	Kritische Schwachstellen in vom Unternehmen genutzter Software müssen zeitnah, spätestens aber 10 Werktage nach der Veröffentlichung einer für diese Schwachstelle relevanten Sicherheitsmaßnahme beseitigt werden. Hierbei sind als kritisch solche Schwachstellen anzusehen, die vom BSI Bundesamt für Sicherheit in der Informationstechnik (Warnstufe hoch oder sehr hoch) oder vom CVSS Common Vulnerability Scoring System als solche benannt bzw. eingestuft wurden (CVSS-Score von mindestens 9,0).		Kritische Schwachstellen in vom Unternehmen genutzter Software müssen zeitnah, spätestens aber 10 Werktage nach der Veröffentlichung einer für diese Schwachstelle relevanten Sicherheitsmaßnahme beseitigt werden. Hierbei sind als kritisch solche Schwachstellen anzusehen, die vom BSI Bundesamt für Sicherheit in der Informationstechnik (Warnstufe hoch oder sehr hoch) oder vom CVSS Common Vulnerability Scoring System als solche benannt bzw. eingestuft wurden (CVSS-Score von mindestens 9,0).		Kritische Schwachstellen in vom Unternehmen genutzter Software müssen zeitnah, spätestens aber 10 Werktage nach der Veröffentlichung einer für diese Schwachstelle relevanten Sicherheitsmaßnahme beseitigt werden. Hierbei sind als kritisch solche Schwachstellen anzusehen, die vom BSI Bundesamt für Sicherheit in der Informationstechnik (Warnstufe hoch oder sehr hoch) oder vom CVSS Common Vulnerability Scoring System als solche benannt bzw. eingestuft wurden (CVSS-Score von mindestens 9,0).		Kritische Schwachstellen in vom Unternehmen genutzter Software müssen zeitnah, spätestens aber 10 Werktage nach der Veröffentlichung einer für diese Schwachstelle relevanten Sicherheitsmaßnahme beseitigt werden. Hierbei sind als kritisch solche Schwachstellen anzusehen, die vom BSI Bundesamt für Sicherheit in der Informationstechnik (Warnstufe hoch oder sehr hoch) oder vom CVSS Common Vulnerability Scoring System als solche benannt bzw. eingestuft wurden (CVSS-Score von mindestens 9,0).	
16	**Patchmanagement**	EoL-/EoS (Altsysteme)	Software, insbesondere Betriebssysteme und Anwendungsprogramme, bei denen der Hersteller den Support eingestellt hat und eine Aktualisierung nicht mehr erfolgen kann (end-of-life / end-of-support), sind spätestens nach 90 Tagen abzulösen oder die entsprechenden Systeme vom restlichen Netz mittels Firewall zu trennen und Zugriffe strikt zu reglementieren. Eine Erreichbarkeit vom Internet ist zu unterbinden.		Software, insbesondere Betriebssysteme und Anwendungsprogramme, bei denen der Hersteller den Support eingestellt hat und eine Aktualisierung nicht mehr erfolgen kann (end-of-life / end-of-support), sind spätestens nach 90 Tagen abzulösen oder die entsprechenden Systeme vom restlichen Netz mittels Firewall zu trennen und Zugriffe strikt zu reglementieren. Eine Erreichbarkeit vom Internet ist zu unterbinden.		Software, insbesondere Betriebssysteme und Anwendungsprogramme, bei denen der Hersteller den Support eingestellt hat und eine Aktualisierung nicht mehr erfolgen kann (end-of-life / end-of-support), sind spätestens nach 90 Tagen abzulösen oder die entsprechenden Systeme vom restlichen Netz mittels Firewall zu trennen und Zugriffe strikt zu reglementieren. Eine Erreichbarkeit vom Internet ist zu unterbinden.		Software, insbesondere Betriebssysteme und Anwendungsprogramme, bei denen der Hersteller den Support eingestellt hat und eine Aktualisierung nicht mehr erfolgen kann (end-of-life / end-of-support), sind spätestens nach 90 Tagen abzulösen oder die entsprechenden Systeme vom restlichen Netz mittels Firewall zu trennen und Zugriffe strikt zu reglementieren. Eine Erreichbarkeit vom Internet ist zu unterbinden.	

Anforderungen an die Cyber-Security zur Versicherbarkeit von Unternehmen

Anforderungskatalog

Nr.	Kriterium	Stichwort		Anforderung	Anforderung	Anforderung
17	Berechtigungen	Grundsatz	Der unbefugte Zugriff auf personenbezogene oder andere kritische Daten wird durch eingeschränkte Berechtigungen verhindert.	Der unbefugte Zugriff auf personenbezogene oder andere kritische Daten wird durch eingeschränkte Berechtigungen - ggf. zusätzlich durch Verschlüsselung - verhindert.	Der unbefugte Zugriff auf personenbezogene oder andere kritische Daten wird durch eingeschränkte Berechtigungen - ggf. zusätzlich durch Verschlüsselung - verhindert.	Der unbefugte Zugriff auf personenbezogene oder andere kritische Daten wird durch eingeschränkte Berechtigungen - ggf. zusätzlich durch Verschlüsselung - verhindert.
18	Berechtigungen	Berechtigungsmanagement		Es sind Verfahren zur Vergabe, Änderung und zum Entzug von Berechtigungen z. B. beim Ausscheiden eines Mitarbeiters in Kraft gesetzt. Vergebene Berechtigungen werden regelmäßig überprüft.	Es sind Verfahren zur Vergabe, Änderung und zum Entzug von Berechtigungen z. B. beim Ausscheiden eines Mitarbeiters in Kraft gesetzt. Vergebene Berechtigungen werden regelmäßig überprüft.	Es sind Verfahren zur Vergabe, Änderung und zum Entzug von Berechtigungen z. B. beim Ausscheiden eines Mitarbeiters in Kraft gesetzt. Vergebene Berechtigungen werden regelmäßig überprüft.
19	Berechtigungen	Passwort-Richtlinie		Für jedes Benutzerkonto muss ein individuelles und komplexes Passwort festgelegt werden (z. B. gemäß Empfehlungen des BSI).	Für jedes Benutzerkonto muss ein individuelles und komplexes Passwort festgelegt werden (z. B. gemäß Empfehlungen des BSI).	Für jedes Benutzerkonto muss ein individuelles und komplexes Passwort festgelegt werden (z. B. gemäß Empfehlungen des BSI).
20	Berechtigungen	Anmeldeversuche		Accounts werden nach einer bestimmten Anzahl von ungültigen Anmeldeversuchen temporär gesperrt.	Accounts werden nach einer bestimmten Anzahl von ungültigen Anmeldeversuchen temporär gesperrt.	Accounts werden nach einer bestimmten Anzahl von ungültigen Anmeldeversuchen temporär gesperrt.
21	Berechtigungen	Privilegierte Accounts		Das Unternehmen verfügt über einen Überblick über alle privilegierten Accounts und hat einen Prozess zu deren Verwaltung etabliert. Dabei werden die Prinzipien need-to-know und least-privilege angewendet.	Das Unternehmen verfügt über einen Überblick über alle privilegierten Accounts und hat einen Prozess zu deren Verwaltung etabliert. Dabei werden die Prinzipien need-to-know und least-privilege angewendet.	Das Unternehmen verfügt über einen Überblick über alle privilegierten Accounts und hat einen Prozess zu deren Verwaltung etabliert. Dabei werden die Prinzipien need-to-know und least-privilege angewendet.
22	Berechtigungen	Nutzungstrennung	Administrative Accounts werden getrennt von regulären Nutzeraccounts und nur für Admin-Tätigkeiten genutzt.	Administrative Accounts werden ausschließlich getrennt von regulären Nutzeraccounts und nur für Admin-Tätigkeiten genutzt.	Administrative Accounts werden ausschließlich getrennt von regulären Nutzeraccounts und nur für Admin-Tätigkeiten genutzt.	Administrative Accounts werden ausschließlich getrennt von regulären Nutzeraccounts und nur für Admin-Tätigkeiten genutzt.
23	Berechtigungen	Sammelaccounts		Es dürfen nur personalisierte administrative Accounts verwendet werden. Für Notfälle können nicht personengebundene administrative Accounts mit komplexen Passwörtern verschlossen vorgehalten werden. Deren Nutzung ist zu dokumentieren.	Es dürfen nur personalisierte administrative Accounts verwendet werden. Für Notfälle können nicht personengebundene administrative Accounts mit komplexen Passwörtern verschlossen vorgehalten werden. Deren Nutzung ist zu dokumentieren.	Es dürfen nur personalisierte administrative Accounts verwendet werden. Für Notfälle können nicht personengebundene administrative Accounts mit komplexen Passwörtern verschlossen vorgehalten werden. Deren Nutzung ist zu dokumentieren.
24	Berechtigungen	Default-Einstellungen		Werksseitig zugewiesene Standard-IDs und -Passwörter sind geändert und mit entsprechend hoher Komplexität versehen.	Werksseitig zugewiesene Standard-IDs und -Passwörter sind geändert und mit entsprechend hoher Komplexität versehen.	Werksseitig zugewiesene Standard-IDs und -Passwörter sind geändert und mit entsprechend hoher Komplexität versehen.
25	Berechtigungen	Cloud-Zugriffe		Administrative Zugänge zu Cloud-Anwendungen sind durch MFA abgesichert.	Administrative Zugänge zu Cloud-Anwendungen sind durch MFA abgesichert.	Administrative Zugänge zu Cloud-Anwendungen sind durch MFA abgesichert.
26	Berechtigungen	Authentifizierung von Admin-Accounts		Administrative Zugänge sind risikogerecht abzusichern (z. B. durch komplexe Passwörter, MFA) und zu überwachen. Über das Internet oder andere unsichere Netze erreichbare Administrationsoberflächen sind mit MFA geschützt.	Administrative Zugänge sind risikogerecht abzusichern (z. B. durch komplexe Passwörter, MFA) und zu überwachen. Über das Internet oder andere unsichere Netze erreichbare Administrationsoberflächen sind mit MFA geschützt.	Administrative Zugänge sind risikogerecht abzusichern (z. B. durch komplexe Passwörter, MFA) und zu überwachen. Über das Internet oder andere unsichere Netze erreichbare Administrationsoberflächen sind mit MFA geschützt.
27	Berechtigungen	Verwaltung von Admin-Accounts		Die Erstellung von neuen oder die Änderung von bestehenden Admin-Accounts ist gegen Missbrauch zu schützen und zu überwachen.	Die Erstellung von neuen oder die Änderung von bestehenden Admin-Accounts ist gegen Missbrauch zu schützen und zu überwachen.	Die Erstellung von neuen oder die Änderung von bestehenden Admin-Accounts ist gegen Missbrauch zu schützen und zu überwachen.
28	Berechtigungen	Domain-Admin-Accounts		Die Anzahl der personalisierten Domain-Admin-Accounts ist auf ein notwendiges Minimum beschränkt (i.d.R. drei bis vier).	Die Anzahl der personalisierten Domain-Admin-Accounts ist auf ein notwendiges Minimum beschränkt (i.d.R. drei bis vier).	Die Anzahl der personalisierten Domain-Admin-Accounts ist auf ein notwendiges Minimum beschränkt (i.d.R. drei bis vier).
29	Berechtigungen	Service Accounts		Sofern Service-Accounts für die Ausführung von Anwendungen und automatisierten Diensten mit privilegierten Rechten bestehen, lassen sich diese nicht für interaktive Logins nutzen und verfügen nicht über Domain-Admin-Rechte. Ausnahmen sind zu begründen und entsprechend gegen Missbrauch abzusichern.	Sofern Service-Accounts für die Ausführung von Anwendungen und automatisierten Diensten mit privilegierten Rechten bestehen, lassen sich diese nicht für interaktive Logins nutzen und verfügen nicht über Domain-Admin-Rechte. Ausnahmen sind zu begründen und entsprechend gegen Missbrauch abzusichern.	Sofern Service-Accounts für die Ausführung von Anwendungen und automatisierten Diensten mit privilegierten Rechten bestehen, lassen sich diese nicht für interaktive Logins nutzen und verfügen nicht über Domain-Admin-Rechte. Ausnahmen sind zu begründen und entsprechend gegen Missbrauch abzusichern.
30	Berechtigungen	Lokale Admin-Rechte		Lokale Admin-Rechte auf Mitarbeiter-Geräten sind deaktiviert oder auf ein notwendiges Minimum beschränkt. Der Zugang zu den lokalen Administrationsrechten wird mit einem sicheren Passwort, das dem User unbekannt ist, geschützt (z. B. über LAPS).	Lokale Admin-Rechte auf Mitarbeiter-Geräten sind deaktiviert oder auf ein notwendiges Minimum beschränkt. Der Zugang zu den lokalen Administrationsrechten wird mit einem sicheren Passwort, das dem User unbekannt ist, geschützt (z. B. über LAPS).	Lokale Admin-Rechte auf Mitarbeiter-Geräten sind deaktiviert oder auf ein notwendiges Minimum beschränkt. Der Zugang zu den lokalen Administrationsrechten wird mit einem sicheren Passwort, das dem User unbekannt ist, geschützt (z. B. über LAPS).

Anforderungskatalog

Nr.	Kriterium	Stichwort		Anforderung	Anforderung	Anforderung
31	Verschlüsselung von Festplatten	Grundsatz		Das Unternehmen stellt sicher, dass Datenspeicher von mobilen Geräten (Laptops, Smartphones, mobile Festplatten etc.) verschlüsselt sind (z. B. mittels Bitlocker), sofern diese schutzbedürftige Daten enthalten und die Geräte außerhalb des Betriebsgeländes genutzt werden.	Das Unternehmen stellt sicher, dass Datenspeicher von mobilen Geräten (Laptops, Smartphones, mobile Festplatten etc.) verschlüsselt sind (z. B. mittels Bitlocker), sofern diese schutzbedürftige Daten enthalten und die Geräte außerhalb des Betriebsgeländes genutzt werden.	Das Unternehmen stellt sicher, dass Datenspeicher von mobilen Geräten (Laptops, Smartphones, mobile Festplatten etc.) verschlüsselt sind (z. B. mittels Bitlocker), sofern diese schutzbedürftige Daten enthalten und die Geräte außerhalb des Betriebsgeländes genutzt werden.
32	BYOD	Grundsatz		Sofern BYOD im Unternehmen zugelassen ist, ist eine Richtlinie dazu für die Mitarbeiter erlassen. Der Zugang zu Unternehmensdaten und -anwendungen sind in geeigneter Weise vor Datenverlust oder Missbrauch geschützt z. B. durch MDM- bzw. Container-Lösungen.	Sofern BYOD im Unternehmen zugelassen ist, ist eine Richtlinie dazu für die Mitarbeiter erlassen. Der Zugang zu Unternehmensdaten und -anwendungen sind in geeigneter Weise vor Datenverlust oder Missbrauch geschützt z. B. durch MDM- bzw. Container-Lösungen.	Sofern BYOD im Unternehmen zugelassen ist, ist eine Richtlinie dazu für die Mitarbeiter erlassen. Der Zugang zu Unternehmensdaten und -anwendungen sind in geeigneter Weise vor Datenverlust oder Missbrauch geschützt z. B. durch MDM- bzw. Container-Lösungen.
33	USB-Ports	Grundsatz		Der Zugriff auf Wechselmedien über USB-Ports ist technisch unterbunden oder auf vom Unternehmen verwaltete Wechselmedien beschränkt.	Der Zugriff auf Wechselmedien über USB-Ports ist technisch unterbunden oder auf vom Unternehmen verwaltete Wechselmedien beschränkt.	Der Zugriff auf Wechselmedien über USB-Ports ist technisch unterbunden oder auf vom Unternehmen verwaltete Wechselmedien beschränkt.
34	Fernzugriffe	Grundsatz	Fernzugriffe sind technisch so abzusichern, dass ein nicht-autorisierter Zugriff verhindert wird (in der Regel zumindest eine VPN-Verbindung mit MFA).	Fernzugriffe sind technisch so abzusichern, dass ein nicht-autorisierter Zugriff verhindert wird (in der Regel zumindest eine VPN-Verbindung mit MFA).	Fernzugriffe sind technisch so abzusichern, dass ein nicht-autorisierter Zugriff verhindert wird (in der Regel zumindest eine VPN-Verbindung mit MFA).	Fernzugriffe sind technisch so abzusichern, dass ein nicht-autorisierter Zugriff verhindert wird (in der Regel zumindest eine VPN-Verbindung mit MFA).
35	Fernzugriffe	Verschlüsselung		Für Fernzugriffe wird stets eine Verschlüsselung nach aktuellem Standard verwendet (VPN, TLS etc.)	Für Fernzugriffe wird stets eine Verschlüsselung nach aktuellem Standard verwendet (VPN, TLS etc.)	Für Fernzugriffe wird stets eine Verschlüsselung nach aktuellem Standard verwendet (VPN, TLS etc.)
36	Fernzugriffe	Fernwartung		Fernwartungszugänge sind objektbezogen beschränkt und - soweit technisch möglich - zusätzlich abzusichern z. B. durch Freischaltung, zeitliche Begrenzung oder Überwachung. Fernwartungen erfolgen nur über verschlüsselte Verbindungen nach aktuellem Standard.	Fernwartungszugänge sind objektbezogen beschränkt und - soweit technisch möglich - zusätzlich abzusichern z. B. durch Freischaltung, zeitliche Begrenzung oder Überwachung. Fernwartungen erfolgen nur über verschlüsselte Verbindungen nach aktuellem Standard.	Fernwartungszugänge sind objektbezogen beschränkt und - soweit technisch möglich - zusätzlich abzusichern z. B. durch Freischaltung, zeitliche Begrenzung oder Überwachung. Fernwartungen erfolgen nur über verschlüsselte Verbindungen nach aktuellem Standard.
37	Fernzugriffe	Mobiles Arbeiten	Zugriffe der Mitarbeiter von außen auf das interne Netzwerk z. B. im Rahmen des mobilen Arbeitens sind zumindest durch VPN mit MFA abgesichert. Dabei kann ein Gerätezertifikat nur dann als zweiter Faktor anerkannt werden, wenn das Gerät selbst als sicher gilt (also vollständig vom Unternehmen gemanagt ist).	Zugriffe der Mitarbeiter von außen auf das interne Netzwerk z. B. im Rahmen des mobilen Arbeitens sind zumindest durch VPN mit MFA abgesichert. Dabei kann ein Gerätezertifikat nur dann als zweiter Faktor anerkannt werden, wenn das Gerät selbst als sicher gilt (also vollständig vom Unternehmen gemanagt ist).	Zugriffe der Mitarbeiter von außen auf das interne Netzwerk z. B. im Rahmen des mobilen Arbeitens sind zumindest durch VPN mit MFA abgesichert. Dabei kann ein Gerätezertifikat nur dann als zweiter Faktor anerkannt werden, wenn das Gerät selbst als sicher gilt (also vollständig vom Unternehmen gemanagt ist).	Zugriffe der Mitarbeiter von außen auf das interne Netzwerk z. B. im Rahmen des mobilen Arbeitens sind zumindest durch VPN mit MFA abgesichert. Dabei kann ein Gerätezertifikat nur dann als zweiter Faktor anerkannt werden, wenn das Gerät selbst als sicher gilt (also vollständig vom Unternehmen gemanagt ist).
38	Fernzugriffe	MDM (Mobile Device Management)			Zur Verwaltung von mobilen Geräten ist ein MDM eingerichtet, welches u.a. die Fernlöschung von Daten ermöglicht.	Zur Verwaltung von mobilen Geräten ist ein MDM eingerichtet, welches u.a. die Fernlöschung von Daten ermöglicht.
39	Netzwerksegmentierung	Grundsatz	Das Netzwerk ist nach jeweiligem Schutzbedarf zu segmentieren.	Das Netzwerk ist nach Schutzbedarf segmentiert. Insbesondere werden Server und Management-Interfaces sowie Backups in jeweils eigene Netzwerksegmente ausgegliedert und Zugriffe darauf beschränkt. Aus dem Internet erreichbare Systeme (z.B. Web- oder E-Mail-Server) sind von vertrauenswürdigen Netzwerk getrennt (z.B. innerhalb einer entmilitarisierten Zone (DMZ) oder bei einem Drittanbieter).	Das Netzwerk ist nach Schutzbedarf segmentiert. Insbesondere werden Server und Management-Interfaces sowie Backups in jeweils eigene Netzwerksegmente ausgegliedert und Zugriffe darauf beschränkt. Aus dem Internet erreichbare Systeme (z.B. Web- oder E-Mail-Server) sind von vertrauenswürdigen Netzwerk getrennt (z.B. innerhalb einer entmilitarisierten Zone (DMZ) oder bei einem Drittanbieter).	Das Netzwerk ist nach Schutzbedarf segmentiert. Insbesondere werden Server und Management-Interfaces sowie Backups in jeweils eigene Netzwerksegmente ausgegliedert und Zugriffe darauf beschränkt. Aus dem Internet erreichbare Systeme (z.B. Web- oder E-Mail-Server) sind von vertrauenswürdigen Netzwerk getrennt (z.B. innerhalb einer entmilitarisierten Zone (DMZ) oder bei einem Drittanbieter).
40	Netzwerksegmentierung	Trennung IT von OT		Das Office-IT-Netzwerk ist von der OT (Produktions- IT/ Medizintechnik/ Gebäudetechnik etc.) getrennt und die Zugriffsrechte strikt reglementiert.	Das Office-IT-Netzwerk ist von der OT (Produktions- IT/ Medizintechnik/ Gebäudetechnik etc.) getrennt und die Zugriffsrechte strikt reglementiert.	Das Office-IT-Netzwerk ist von der OT (Produktions- IT/ Medizintechnik/ Gebäudetechnik etc.) getrennt und die Zugriffsrechte strikt reglementiert.
41	Netzwerksegmentierung	technische Umsetzung		Die Segmentierung erfolgt physisch oder über Firewall-Einstellungen.	Die Segmentierung erfolgt physisch oder über Firewall-Einstellungen.	Die Segmentierung erfolgt physisch oder über Firewall-Einstellungen.
42	Netzwerksegmentierung	WLAN		Sofern ein Gast-WLAN-Zugang eingerichtet ist, ist hierfür ein gesondertes, vom Firmennetzwerk getrenntes und verschlüsseltes WLAN eingerichtet.	Sofern ein Gast-WLAN-Zugang eingerichtet ist, ist hierfür ein gesondertes, vom Firmennetzwerk getrenntes und verschlüsseltes WLAN eingerichtet.	Sofern ein Gast-WLAN-Zugang eingerichtet ist, ist hierfür ein gesondertes, vom Firmennetzwerk getrenntes und verschlüsseltes WLAN eingerichtet.

Anforderungskatalog

Nr.	Kriterium	Stichwort		Anforderung	Anforderung	Anforderung
43	Detektion und Reaktion	Grundsatz	Das Unternehmen verfügt über technische Schutzmaßnahmen gegen unbefugten Zugriff durch Firewalls und Virenscanner, die automatisch aktualisiert werden.	Das Unternehmen verfügt über technische Schutzmaßnahmen gegen unbefugten Zugriff durch Firewalls und Virenscanner, die automatisch aktualisiert werden.	Das Unternehmen verfügt über technische Schutzmaßnahmen gegen unbefugten Zugriff durch Firewalls und Virenscanner, die automatisch aktualisiert werden.	Das Unternehmen verfügt über technische Schutzmaßnahmen gegen unbefugten Zugriff durch Firewalls und Virenscanner, die automatisch aktualisiert werden.
44	Detektion und Reaktion	Firewalls		Alle Internetzugänge sind durch eine Firewall geschützt, die so konfiguriert ist, dass nur erforderliche Dienste zugelassen sind.	Alle Internetzugänge sind durch eine Firewall geschützt, die so konfiguriert ist, dass nur erforderliche Dienste zugelassen sind.	Alle Internetzugänge sind durch eine Firewall geschützt, die so konfiguriert ist, dass nur erforderliche Dienste zugelassen sind.
45	Detektion und Reaktion	IDS und IPS		Auf allen Firewalls zur Absicherung der Zugänge zum Internet ist mindestens IDS, möglichst auch Intrusion Prevention System (IPS) aktiviert.	Auf allen Firewalls zur Absicherung der Zugänge zum Internet ist mindestens IDS, möglichst auch Intrusion Prevention System (IPS) aktiviert.	Auf allen Firewalls zur Absicherung der Zugänge zum Internet ist ein Intrusion Prevention System (IPS) aktiviert.
46	Detektion und Reaktion	Blocken von RDP		Firewalls sind so eingestellt, dass die Verwendung von RDP (Remote-Desktop-Protokoll) von außen verhindert wird.	Firewalls sind so eingestellt, dass die Verwendung von RDP (Remote-Desktop-Protokoll) verhindert wird.	Firewalls sind so eingestellt, dass die Verwendung von RDP (Remote-Desktop-Protokoll) verhindert wird.
47	Detektion und Reaktion	Verhaltensbasierter Schutz		Das Unternehmen setzt - soweit technisch möglich - eine verhaltensbasierte Schutzsoftware auf allen Servern und Clients ein.	Das Unternehmen setzt - soweit technisch möglich - eine verhaltensbasierte Schutzsoftware auf allen Servern und Clients ein.	Das Unternehmen setzt - soweit technisch möglich - eine verhaltensbasierte Schutzsoftware auf allen Servern und Clients ein.
48	Detektion und Reaktion	EDR (Endpoint Detection & Response)		Auf allen Servern und soweit möglich auch allen Clients sind EDR bzw. XDR-Lösungen aktiviert	Auf allen Servern und soweit möglich auch allen Clients sind EDR bzw. XDR-Lösungen aktiviert	Auf allen Servern und soweit möglich auch allen Clients sind EDR bzw. XDR-Lösungen aktiviert
49	Detektion und Reaktion	Log-Files		Es werden Event-Logs aus Identitätsdiensten (z.B. AD, Server u. Clients), Firewalls und sonstigen Sicherheitssystemen zur Analyse von möglichen Sicherheitsvorfällen generiert und über mind. 3 Monate gespeichert.	Es werden Event-Logs aus Identitätsdiensten (z.B. AD, Server u. Clients), Firewalls und sonstigen Sicherheitssystemen zur Analyse von möglichen Sicherheitsvorfällen generiert und über mind. 3 Monate gespeichert.	Es werden Event-Logs aus Identitätsdiensten (z.B. AD, Server u. Clients), Firewalls und sonstigen Sicherheitssystemen zur Analyse von möglichen Sicherheitsvorfällen generiert und über mind. 3 Monate gespeichert.
50	Detektion und Reaktion	Reaktion		Es ist sichergestellt, dass Meldungen über potentielle Sicherheitsvorfälle spätestens bis zum nächsten Werktag bewertet und darauf reagiert wird.	Es ist sichergestellt, dass Meldungen über potentielle Sicherheitsvorfälle spätestens bis zum nächsten Werktag bewertet und darauf reagiert wird.	Es ist sichergestellt, dass Meldungen über potentielle Sicherheitsvorfälle innerhalb von 24 h bewertet und darauf reagiert wird.
51	Detektion und Reaktion	SIEM		Das Unternehmen hat Tools und Prozesse zur Erkennung und Dokumentierung von Auffälligkeiten in den internen Netzwerken etabliert, um Security-Incidents frühzeitig erkennen zu können.	Das Unternehmen hat Tools und Prozesse zur Erkennung und Dokumentierung von Auffälligkeiten in den internen Netzwerken etabliert, um Security-Incidents frühzeitig erkennen zu können.	Das Unternehmen hat Tools und Prozesse zur Erkennung und Dokumentierung von Auffälligkeiten in den internen Netzwerken etabliert, um Security-Incidents frühzeitig erkennen zu können.
52	Detektion und Reaktion	Security Operation Center (SOC)		Das Unternehmen verfügt über ein SOC für alle kritischen Unternehmensbereiche	Das Unternehmen verfügt über ein SOC für alle kritischen Unternehmensbereiche	Das Unternehmen verfügt über ein SOC für alle kritischen Unternehmensbereiche
53	Backup	Häufigkeit	Das Unternehmen sichert seine betriebskritischen Systeme und Daten risikoadäquat in angemessenen Abständen (in der Regel werktäglich).	Das Unternehmen sichert seine betriebskritischen Systeme und Daten risikoadäquat in angemessenen Abständen (in der Regel werktäglich).	Das Unternehmen sichert seine betriebskritischen Systeme und Daten risikoadäquat in angemessenen Abständen (in der Regel werktäglich).	Das Unternehmen sichert seine betriebskritischen Systeme und Daten risikoadäquat in angemessenen Abständen (in der Regel werktäglich).
54	Backup	Historizität		Es werden Sicherungen vorgehalten, die zeitlich mindestens drei Monate in die Vergangenheit reichen.	Es werden Sicherungen vorgehalten, die zeitlich mindestens drei Monate in die Vergangenheit reichen. Es sind RPOs (Recovery Point Objektives) definiert für alle kritischen Daten.	Es werden Sicherungen vorgehalten, die zeitlich mindestens drei Monate in die Vergangenheit reichen. Es sind RPOs (Recovery Point Objektives) definiert für alle kritischen Daten.
55	Backup	Sichere Speicherung	Sicherungsdatenträger werden so aufbewahrt, dass sie nicht vom selben Schadenereignis wie die Original-Dateien betroffen werden können (in der Regel "Offline-Sicherung"). Sofern eine Offline-Sicherung nicht erfolgt, muss zumindest eine Aufbewahrung außerhalb der Domain und vor Manipulation geschützt erfolgen.	Sicherungsdatenträger werden so aufbewahrt, dass sie nicht vom selben Schadenereignis wie die Original-Dateien betroffen werden können (in der Regel "Offline-Sicherung"). Sofern eine Offline-Sicherung nicht erfolgt, muss zumindest eine Aufbewahrung außerhalb der Domain und vor Manipulation geschützt erfolgen.	Sicherungsdatenträger werden so aufbewahrt, dass sie nicht vom selben Schadenereignis wie die Original-Dateien betroffen werden können (in der Regel "Offline-Sicherung"). Sofern eine Offline-Sicherung nicht erfolgt, muss zumindest eine Aufbewahrung außerhalb der Domain und vor Manipulation geschützt erfolgen.	Sicherungsdatenträger werden so aufbewahrt, dass sie nicht vom selben Schadenereignis wie die Original-Dateien betroffen werden können (in der Regel "Offline-Sicherung"). Sofern eine Offline-Sicherung nicht erfolgt, muss zumindest eine Aufbewahrung außerhalb der Domain und vor Manipulation geschützt erfolgen.
56	Backup	Rücksicherbarkeit		Form und Struktur der Daten auf dem Sicherungsdatenträger sind so beschaffen, dass deren Rücksicherung technisch möglich ist. Die Ausführung des Backups wird überwacht.	Form und Struktur der Daten auf dem Sicherungsdatenträger sind so beschaffen, dass deren Rücksicherung technisch möglich ist. Die Ausführung des Backups wird überwacht.	Form und Struktur der Daten auf dem Sicherungsdatenträger sind so beschaffen, dass deren Rücksicherung technisch möglich ist. Die Ausführung des Backups wird überwacht.
57	Backup	Restore-Tests		Die Rücksicherbarkeit von Backups wird mindestens jährlich überprüft.	Die Rücksicherbarkeit von Backups wird mindestens jährlich überprüft.	Die Rücksicherbarkeit von Backups wird mindestens jährlich überprüft.

Anforderungen an die Cyber-Security zur Versicherbarkeit von Unternehmen

Anforderungskatalog

Nr.	Kriterium	Stichwort		Anforderung	Anforderung	Anforderung
58	Notfallmanagement	Grundsatz	Das Unternehmen verfügt über einen aktuellen Notfallplan für Sicherheitsvorfälle - insbesondere für das Szenario Cyber-Angriff / Ransomware. Hierin enthalten sind u.a. Sofortmaßnahmen, Verantwortlichkeiten, Kontaktdaten sowie ein Wiederanlaufplan.	Das Unternehmen verfügt über einen aktuellen Notfallplan für Sicherheitsvorfälle - insbesondere für das Szenario Cyber-Angriff / Ransomware. Hierin enthalten sind u.a. Sofortmaßnahmen, Verantwortlichkeiten, Kontaktdaten sowie ein Wiederanlaufplan.	Das Unternehmen verfügt über einen aktuellen Notfallplan für Sicherheitsvorfälle - insbesondere für das Szenario Cyber-Angriff / Ransomware. Hierin enthalten sind u.a. Sofortmaßnahmen, Verantwortlichkeiten, Kontaktdaten sowie ein Wiederanlaufplan.	Das Unternehmen verfügt über einen aktuellen Notfallplan für Sicherheitsvorfälle - insbesondere für das Szenario Cyber-Angriff / Ransomware. Hierin enthalten sind u.a. Sofortmaßnahmen, Verantwortlichkeiten, Kontaktdaten sowie ein Wiederanlaufplan.
59	Notfallmanagement	Verfügbarkeit	Der Notfallplan steht auch bei einem Ausfall der IT z. B. durch physische Ablage zur Verfügung.	Der Notfallplan steht auch bei einem Ausfall der IT z. B. durch physische Ablage zur Verfügung.	Der Notfallplan steht auch bei einem Ausfall der IT z. B. durch physische Ablage zur Verfügung.	Der Notfallplan steht auch bei einem Ausfall der IT z. B. durch physische Ablage zur Verfügung.
60	Notfallmanagement	Aktualisierung		Der Notfallplan wird jährlich auf Aktualität überprüft.	Der Notfallplan wird jährlich auf Aktualität überprüft.	Der Notfallplan wird jährlich auf Aktualität überprüft.
61	Notfallmanagement	Notfall-Übungen			Die Wirksamkeit des Notfallplans wird mind. alle drei Jahre durch eine Übung überprüft.	Die Wirksamkeit des Notfallplans wird mind. alle drei Jahre durch eine Übung überprüft.
62	Betrugs-Prävention (sofern mitversichert)	4-Augen-Prinzip	Bei Überweisungen von mehr als 10.000 EUR ist ein 4-Augen-Prinzip anzuwenden und zu dokumentieren.	Bei Überweisungen von mehr als 10.000 EUR ist ein 4-Augen-Prinzip anzuwenden und zu dokumentieren.	Bei Überweisungen von mehr als 20.000 EUR ist ein 4-Augen-Prinzip anzuwenden und zu dokumentieren.	Bei Überweisungen von mehr als 25.000 EUR ist ein 4-Augen-Prinzip anzuwenden und zu dokumentieren.
63	Management	Verantwortung		Die Geschäftsführung hat eine für Informationssicherheit verantwortliche Person benannt, die über ausreichend Kenntnisse hierzu verfügt.	Die Geschäftsführung hat eine für Informationssicherheit verantwortliche Person benannt, die über ausreichend Kenntnisse und Ressourcen hierzu verfügt.	Die Geschäftsführung hat eine für Informationssicherheit verantwortliche Person benannt, die über ausreichend Kenntnisse und Ressourcen hierzu verfügt.
64	Management	ISMS (Informationssicherheitsmanagementsystem)			Das Unternehmen hat ein ISMS dokumentiert und eingeführt.	Das Unternehmen hat ein ISMS dokumentiert und eingeführt.
65	Management	Zertifizierung				Das ISMS ist nach einem anerkannten Standard zertifiziert
66	Management	Maßnahmenpläne			Es werden mindestens jährlich Maßnahmen zur Verbesserung der Informationssicherheit im Unternehmen festgelegt und von der obersten Leitung freigegeben.	Es werden mindestens jährlich Maßnahmen zur Verbesserung der Informationssicherheit im Unternehmen festgelegt und von der obersten Leitung freigegeben.
67	Management	Risikomanagement			Es werden mindestens jährlich Risikoberichte zur Informations- und Cybersicherheit der obersten Leitung vorgelegt.	Es werden mindestens jährlich Risikoberichte zur Informations- und Cybersicherheit der obersten Leitung vorgelegt.
68	Management	Lieferantenmanagement		Anforderungen an IT-Dienstleister werden bezüglich Informationssicherheit, Vertraulichkeit und Datenschutz vertraglich geregelt und vom Unternehmen überwacht.	Anforderungen an IT-Dienstleister werden bezüglich Informationssicherheit, Vertraulichkeit und Datenschutz vertraglich geregelt und vom Unternehmen überwacht. Schwerwiegende Sicherheitsvorfälle beim Dienstleister müssen dem Unternehmen unverzüglich gemeldet werden.	Anforderungen an IT-Dienstleister werden bezüglich Informationssicherheit, Vertraulichkeit und Datenschutz vertraglich geregelt und vom Unternehmen überwacht. Schwerwiegende Sicherheitsvorfälle beim Dienstleister müssen dem Unternehmen unverzüglich gemeldet werden.
69	Management	Fremdpersonen		Sofern fremde Personen auf dem Betriebsgelände Zugang haben und sich mit eigenen Geräten in das Netzwerk einloggen (z. B. Wartungspersonal, externe IT-Dienstleister), müssen diese Geräte vorab einer Security-Prüfung unterzogen werden.	Sofern fremde Personen auf dem Betriebsgelände Zugang haben und sich mit eigenen Geräten in das Netzwerk einloggen (z. B. Wartungspersonal, externe IT-Dienstleister), müssen diese Geräte vorab einer Security-Prüfung unterzogen werden.	Sofern fremde Personen auf dem Betriebsgelände Zugang haben und sich mit eigenen Geräten in das Netzwerk einloggen (z. B. Wartungspersonal, externe IT-Dienstleister), müssen diese Geräte vorab einer Security-Prüfung unterzogen werden.
70	Management	Due Diligence			Es sind Prozesse definiert, wie neu hinzukommende Unternehmen in die IT-Infrastruktur und Sicherheitsrichtlinien integriert werden. Netzwerke werden erst dann integriert, wenn ein vergleichbares Sicherheitsniveau erreicht ist.	Es sind Prozesse definiert, wie neu hinzukommende Unternehmen in die IT-Infrastruktur und Sicherheitsrichtlinien integriert werden. Netzwerke werden erst dann integriert, wenn ein vergleichbares Sicherheitsniveau erreicht ist.
71	Datenschutz	Datenschutzrichtlinie		Das Unternehmen hat eine Richtlinie erlassen zum Umgang mit personenbezogenen Daten, u.a. bezüglich des Web-Auftritts. Die Richtlinie wird regelmäßig aktualisiert.	Das Unternehmen hat eine Richtlinie erlassen zum Umgang mit personenbezogenen Daten, u.a. bezüglich des Web-Auftritts. Die Richtlinie wird regelmäßig aktualisiert.	Das Unternehmen hat eine Richtlinie erlassen zum Umgang mit personenbezogenen Daten, u.a. bezüglich des Web-Auftritts. Die Richtlinie wird regelmäßig aktualisiert.
72	Datenschutz	Datenschutz-Audits			Das Unternehmen führt regelmäßig Audits zum Stand der Umsetzung von gesetzlich geforderten Datenschutzmaßnahmen durch und berichtet gegenüber der obersten Leitung.	Das Unternehmen führt regelmäßig Audits zum Stand der Umsetzung von gesetzlich geforderten Datenschutzmaßnahmen durch und berichtet gegenüber der obersten Leitung.