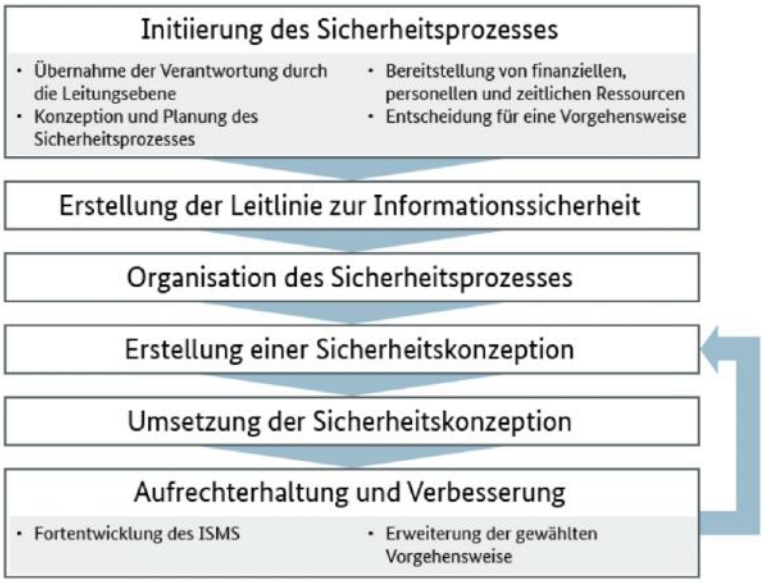
10_ITT_22-23_S120-126_Themengebiet4

Donnerstag, 20. Juli 2023 21:18

4.4 Schutzbedarfsfeststellung

4.4.1 Phasen des Sicherheitsprozesses nach BSI

Für einen effizienten und geordneten Sicherheitsprozess empfiehlt das BSI folgende Vorgehensweise.



Quelle: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_2_Sicherheitsmanagement/Lektion_2_02/Lektion_2_02_node.html

1. Schritt: Sicherheitsleitlinie

Die Erstellung einer Sicherheitsleitlinie ist dabei das wichtigste **Grundsatzdokument**. In diesem wird der Stellenwert der Informationssicherheit für das ganze Unternehmen und allen Beteiligten in Bezug auf verbindliche Prinzipien, auf das anzustrebende Niveau und die gesetzten Ziele formuliert. Dabei findet auch der organisatorische Rahmen Berücksichtigung. Hierbei sollte auch klar geregelt werden, welche Folgen Verstöße haben.

2. Schritt: Sicherheitskonzept

Das Sicherheitskonzept bezieht sich auf die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten als Erstaufnahme. Man spricht hierbei auch von einem **Informationsverbund**. Dabei bezieht sich das Sicherheitskonzept ganz allgemein auf die TOM (s. Abschnitt zuvor). Folgendes sollte bei der Zusammenstellung des Sicherheitskonzeptes überprüft werden, ob diese Angaben enthalten sind:

- Geschäftsprozesse im Informationsverbund (Name, Beschreibung, fachverantwortliche Stelle)
- Anwendungen in diesen Prozessen (Bezeichnung und Beschreibungen),
- IT-Systeme und ICS-Komponenten[2] (Bezeichnung und Beschreibung)
- Für den Informationsverbund wichtige Räume, z.B. Serverraum (Art, Raumnummer und Gebäude).
- Virtuelle Systeme (entsprechend gekennzeichnet und benannt).

Ein grafischer Netzplan mit der Darstellung der Vernetzung der Geräte bzw. Zielobjekte wird empfohlen.

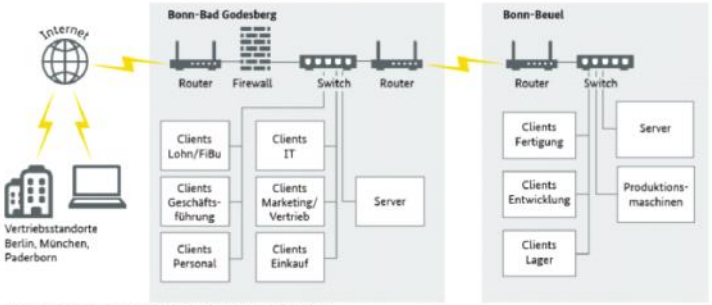


Abbildung 2: Netzplan der RECPLAST GmbH – Übersicht

Quelle:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Webkurs/Recplast_Onlinekurs2018.pdf%3F__blob%3DpublicationFile%26v%3D7, S. 14

[2] Industrial Control System, ist ein Oberbegriff für Automatisierungslösungen zur Steuerung technischer Prozesse.

3. Schritt: Strukturanalyse

Hierbei werden die bisher gesammelten Informationen systematisch aufbereitet. Die Ergebnisse der Erstaufnahme werden nun vervollständigt. Dies zeigt das folgende Beispiel vom BSI aus dem Beispielunternehmen der *RECPLAST GmbH* zur Erfassung der **Geschäftsprozesse**, **Anwendungen** und **Informationen**.

Geschäftsprozesse

Bezeichnung	Name und Beschreibung des Prozesses	Prozess-Verantwortlicher	Mitarbeiter
GP001	**Produktion (Kerngeschäft):** Die Produktion der Kunststoffartikel umfasst alle Phasen von der Materialbereitstellung bis zur Einlagerung des produzierten Materials. Hierzu gehören innerhalb der Produktion die internen Transportwege, die Produktion und Fertigung der verschiedenen Komponenten und das Verpacken der Teile. Es werden alle Informationen über Aufträge, Lagerbestände und Stücklisten verarbeitet.	Leiter Produktion	Alle Mitarbeiter
GP002	**Angebotswesen (unterstützender Prozess):** In der Angebotsabwicklung werden die Kundenanfragen für Produkte verarbeitet. Im Regelfall werden Kundenanfragen formlos per E-Mail oder Fax geschickt. Die Angebote werden elektronisch erfasst und ein schriftliches Angebot per Post an den Kunden versendet. Im Angebotswesen werden Kundendaten, Lagerbestände, Anfragen und Angebote bearbeitet.	Leiter Angebotswesen	Vertrieb

Übersicht Geschäftsprozesse, Quelle:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Webkurs/Recplast_Onlinekurs2018.pdf%3F__blob%3DpublicationFile%26v%3D7, S. 12

Anwendungen

Bezeich-nung	Name und Beschreibung der Anwendung	Anzahl	Benutzer	Verantwortlich/ Administrator
A001	**Textverarbeitung, Präsentation, Tabellenkalkulation:** Alle geschäftlichen Informationen werden in einem Office-Produkt verarbeitet, Geschäftsbriefe, Analysen oder Präsentationen.	290	Alle Mitarbeiter	IT-Betrieb
A002	**Lotus Notes:** Diese Anwendung wird von allen Mitarbeitern für die Bearbeitung von Mailnachrichten, Terminen und Kontakten genutzt.	290	Alle Mitarbeiter	IT-Betrieb
A003	**Internet-Recherche**	290	Alle Mitarbeiter	IT-Betrieb
A004	**Prozessleitsystem:** zur Steuerung der SPS-Systeme	1	Produktion	Leiter Produktion
A005	**Entwicklungssystem:** zur Entwicklung von SPS-Programmierungen	75	Entwicklung	Leiter Produktion

Übersicht Anwendungen, Quelle:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Webkurs/Recplast_Onlinekurs2018.pdf%3F__blob%3DpublicationFile%26v%3D7, S. 12

IT -Systeme

Nr.	Beschreibung	Plattform	Standort	Anzahl	Benutzer/Administrator
S001	Domänen-Controller (virtualisiert)	Windows Server 2012	Bad Godesberg, R. 1.02 (Serverraum) Beuel, R. 2.01 (Serverraum)	2	Alle IT-Benutzer/ IT-Administration
S002	Dateiserver (virtualisiert)	Windows Server 2012	Bad Godesberg, R. 1.02 (Serverraum) Beuel, R. 2.01 (Serverraum)	2	Alle IT-Benutzer/ IT-Administration
S003	Druckserver (virtualisiert)	Windows Server 2012	Bad Godesberg, R. 1.02 (Serverraum) Beuel, R. 2.01 (Serverraum)	2	Alle IT-Benutzer/ IT-Administration

Übersicht Server, Quelle:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Webkurs/Recplast_Onlinekurs2018.pdf%3F__blob%3DpublicationFile%26v%3D7, S. 16

Nr.	Beschreibung	Plattform	Standort	Anzahl	Benutzer/Administrator
C1	Desktops der Finanzbuchhaltung	Windows 10	BG, R. 2.10 – 2.12	30	Mitarbeiter in der Finanzbuchhaltung IT-Administration
C2	Desktops der Geschäftsführung	Windows 10	BG, R. 1.10 – 1.13	15	Geschäftsführung/ IT-Administration
C3	Desktops der Personalabteilung	Windows 10	BG, R. 1.07 – 1.09	15	Mitarbeiter der Personalabteilung/ IT-Administration

Übersicht Clients, Quelle:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Webkurs/Recplast_Onlinekurs2018.pdf%3F__blob%3DpublicationFile%26v%3D7, S. 16

Nr.	Beschreibung	Plattform	Standort	Anzahl	Benutzer/Administrator
N1	Router zum Internet	DSL-Router	Bad Godesberg, R. 1.02 (Serverraum)	1	Alle IT-Benutzer/ IT-Administration
N2	Firewall		Bad Godesberg, R. 1.02 (Serverraum)	1	Alle IT-Benutzer/ IT-Administration
N3	Zentrale Switche in Bad Godesberg und Beuel		Bad Godesberg, R. 1.02 (Serverraum) Beuel, R. 2.01 (Serverraum)	2	Alle IT-Benutzer/ IT-Administration
N4	Router zur Verbindung der Standorte Bad Godesberg und Beuel		Bad Godesberg, R. 1.02 (Serverraum) Beuel, R. 2.01 (Serverraum)	2	Alle IT-Benutzer/ IT-Administration

Übersicht Netz- und Telekommunikationskomponenten, Quelle:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Webkurs/Recplast_Onlinekurs2018.pdf%3F__blob%3DpublicationFile%26v%3D7, S. 19

Räume

Gebäude/Raum				IT-Komponenten
Kürzel	**Bezeichnung**	**Art**	**Lokation**	**IT-Systeme**
GB1	Verwaltungsgebäude	Gebäude	Bonn-Bad Godesberg	
GB2	Produktionsgebäude	Gebäude	Bonn-Beuel	
R001	Technikraum Bad Godesberg (BG, R. 1.01)	Technikraum	GB1	T1
R002	Serverraum Bad Godesberg (BG, R. 1.02)	Serverraum	GB1	S001 bis S007 N1 bis N4
R003	Büros IT-Abteilung (BG, R. 1.03 – 1.06)	Büroräume	GB1	C4, L4
R004	Büros Personalabteilung (BG, R. 1.07 – 1.09)	Büroräume	GB1	C3, L3
R005	Büros Geschäftsführung (BG, R. 1.10 – 1.13)	Büroräume	GB1	C2, L2

Übersicht Räume und Gebäude, Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Webkurs/Recplast_Onlinekurs2018.pdf%3F__blob%3DpublicationFile%26v%3D7, S. 20f.

Verknüpfungen

Geschäftsprozess	Anwendung									
	A001	**A002**	**A003**	**A004**	**A005**	**A006**	**A007**	**A008**	**A009**	**A010**
GP001	X			X	X				X	X
GP002	X	X	X	X					X	X
GP003	X	X		X				X	X	X
GP004	X	X	X					X		X
GP005	X	X	X	X				X	X	X

Zuordnung Anwendungen und Geschäftsprozesse, Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Webkurs/Recplast_Onlinekurs2018.pdf%3F__blob%3DpublicationFile%26v%3D7, S. 20f.

Nr.	Beschreibung	S001	S002	S003	S004	S005	S006	S007	S008
A001	Office-Anwendungen		X					X	
A002	E-Mail und Terminkalender	X			X			X	
A003	Internet-Recherche		X					X	
A004	Prozessleitsystem								X
A005	Entwicklungssystem		X					X	
A006	Personaldatenverarbeitung	X						X	

Verknüpfung Anwendung und Servern, Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Webkurs/Recplast_Onlinekurs2018.pdf%3F__blob%3DpublicationFile%26v%3D7, S. 17

Nr.	Beschreibung	C1	C2	C3	C4	C5	C6	C7	C8	C9
A001	Office-Anwendungen	X	X	X	X	X	X	X	X	X
A002	E-Mail und Terminkalender	X	X	X	X	X	X	X	X	X
A003	Internet-Recherche	X	X	X	X	X			X	X
A004	Prozessleitsystem						X	X		
A005	Entwicklungssystem						X	X		
A006	Personaldatenverarbeitung		X	X						
A007	Reisekostenabrechnung			X						
A008	Finanzbuchhaltung	X	X							

Verknüpfung Anwendung und Clients, Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Webkurs/Recplast_Onlinekurs2018.pdf%3F__blob%3DpublicationFile%26v%3D7, S. 18

Nr.	Beschreibung	N1	N2	N3	N4	T1	T2
A001	Office-Anwendungen			X	X		
A002	E-Mail und Terminkalender	X	X	X	X		
A003	Internet-Recherche	X	X	X	X		
A004	Prozessleitsystem			X	X		
A005	Entwicklungssystem			X	X		
A006	Personaldatenverarbeitung			X			
A007	Reisekostenabrechnung			X			

Verknüpfung Anwendung und Netz- und Telekommunikationskomponenten, Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Webkurs/Recplast_Onlinekurs2018.pdf%3F__blob%3DpublicationFile%26v%3D7, S. 20f.

4. Schritt: Schutzbedarfsfeststellung

Nun ist im letzten Schritt zu klären, wie viel Schutz Informationen, Anwendungen und die dazugehörigen technischen Systeme und Infrastrukturkomponenten benötigen. Dabei ist zu prüfen und zu begründen, welche Komponenten mehr Sicherheit benötigen und wann elementare Schutzmaßnahmen genügen.

4.4.2 Schutzbedarfsfeststellung durchführen

Arbeitsauftrag

Führen Sie nun selbstständig eine Schutzbedarfsfeststellung am Beispiel „Fax" durch. Nutzen Sie dazu das IT-Grundschutz-Kompendium des BSI. (**Hinweis**: Raum 001 ist ein Großraumbüro, Raum 002 ist das Büro des Abteilungsleiters)

Nr.	Grundwert	Schutzbedarf	Begründung	Maßnahmen
Fax F.7 Raum 001	Vertraulichkeit	sehr hoch	im Großraumbüro können Unbefugte leichter Einsicht in schützenswerte Daten erhalten, da Fax für alle zugänglich ist	• nur berechtigte Personen im Büro erhalten Zugriff auf Fax(z.B. durch einschließen) • ggf. Einsatz eines abgesicherten Fax-Servers anstelle eines analogen Fax • Zugriff auf Fax protokollieren → nur angemeldete Benutzer können die Empfangenen Faxe angucken
	Integrität	normal	Fehlerhafte Übertragung, falscher Absender möglich, aber in DE hohe Wertigkeit	
	Verfügbarkeit	hoch	Fax wird von vielen MA genutzt	
Fax F.6 Raum 002	Vertraulichkeit	normal	Zugang hat nur eine berechtigte Person (Abteilungsleiter)	entsprechende Regeln, dass weitere Personen (Hausmeister, Putzdienst) keine Einsicht bekommen. z.B. wegsperren nach Feierabend
	Integrität	normal	Fehlerhafte Übertragung, falscher Absender möglich, aber in DE hohe "Wertigkeit durch Gerichtsurteil"	
	Verfügbarkeit	normal	Fax wird nur von einem MA genutzt	