Wo sind unsere Daten ?

" CYBER-SECURITY IST KEINE MAGIE "
Jan Volkmann

Projektabschlußarbeit Klasse 2
2023

Team Patrick Müller Steve Meissner Jan Volkmann

Quelle Bild https://pixabay.com/de/illustrations/gehackt-cyberkriminalit%c3%a4t-rechner-2127635/

Inhaltsverzeichnis

Glossar

Netzplan	Ist die grafische Darstellung aller Geräte im Netzwerk mit den notwendigen Verbindungen
Strukturanalyse	Ist eine Bestandsaufnahme des Ist-Zustandes einer Firma, wo alle Geräte und Prozesse aufgenommen werden
Modellierung	ist die Ermittlung der Bausteine für die Umsetzung. Dabei ist das BSI-Grundschutzkompendium die Vorlage
Berechtigungskonzept	Das Berechtigungskonzept legt fest, ob ein Nutzer auf eine Anwendung nur Leserechte, Schreib- und Leserechte oder keine Rechte erhält
IT-Grundschutz-Check	Der Grundschutz-Check ist meist am Ende. Dort vergleicht man die Anforderungen, mit dem aktuellen Zustand. Dabei sollten überall erfüllt stehen und wenn nur teilweise, dann auch Grund
Netzwerk	Gesamtheit aller Geräte, die miteinander verbunden sind
Windows Active Directory	Die Windows Active Directory ist eine Netzwerkumgebung, in der sich alle Benutzer anmelden, und dann dadurch Ihre Rechte zugewiesen bekommen
BSI-Grundschutzkompendium	in diesem Werk finden wir alles wissenswertes zum Schutz zum Thema Informationssicherheit. Für sehr viel existieren Bausteine, anhand der vorgeschlagenen Lösungen, orientiert man sich sehr gut
IT- Infrastruktur,-Komponenten	Informationstechnik und Einzelteil in einem Netzwerk
BSI-Grundschutz	Der BSI-Grundschutz ist der Einstieg in die Absicherung einer Firma
Exchange Server	Anwendung die für die Verarbeitung der E-Mail zuständig ist Von der Firma Microsoft
Fido Key	Hardware USB-Stick, der nur für die Autorisierung zuständig ist und in verschiedenen Anwendungen zur sicheren Authentifizierung genutzt werden kann
Failover	meist in Verbindung mit Internetzugang. Es existiert eine Ersatzleitung, die jederzeit, die Hauptleitung ersetzen kann, wenn diese ausfällt
USV-Lösung	Universelle Stromversorgung, die bei Ausfall der Stromversorgung diese blitzschnell ersetzt und das System noch eine gewisse Zeit am Laufen hält
ERP-Anwendung	Anwendung, womit der Vertrieb meist arbeitet

Abkürzungsverzeichnis

BSI	Bundesamt für Sicherheit
ISB	Informationssicherheitsbeauftragter
IT-Admins	Systemadministrator für alle Geräte im Netzwerk
AD	Ist meist die Kurzform zu Windows Active Directory
OWA	Office Web Applikation, Bestandteil des Exchange Servers
LTE	schnelles mobiles Internet (Long Term Evolution Standard)
Sandbox	gesicherte Umgebung, mit gefahrloser Testmöglichkeit
Multifaktor	zusätzliches Sicherheitsmerkmal zu Benutzer und Passwort

1. Einleitung

1.1 Projektumfeld

Super Sound ist ein deutsches Unternehmen mit Sitz in Unna, das im Jahr 2005 gegründet wurde und sich auf die Herstellung und den Vertrieb von Produkten für den exzellenten Klang im Auto spezialisiert hat. Das Unternehmen beschäftigt 22 Mitarbeiter und hat sich auf die Exklusivmarke "Sound Dreams" konzentriert.
Alle Produkte von Super Sound werden in Deutschland hergestellt und entsprechen einem hohen Qualitätsstandard. Die Firma ist ISO 9001 zertifiziert und hat auch einen Datenschutzbeauftragten. Das Unternehmen vertreibt Geräte, Soundsysteme, Einzelteile und Zubehör für alle Automarken. Die Kunden von Super Sound sind vielfältig und beinhalten auch viele Prominente.
Super Sound ist bekannt für seinen exzellenten Kundenservice und geht sehr kulant mit seinen Kunden um. Das Unternehmen ist bestrebt, seinen Kunden den bestmöglichen Klang im Auto zu bieten und sorgt dafür, dass seine Produkte den höchsten Standards entsprechen. Mit der exklusiven Marke "Sound Dreams" bietet Super Sound seinen Kunden exklusiven Sound vom Feinsten in ihrem Auto.

1.2 Projektziel

Der Chef der Firma „Super Sound „macht sich Gedanken um die Sicherheit seines Unternehmens gegenüber Cyber-Angriffen. Er hat in seiner Firma schon 2018 eine gewisse Sicherheit umgesetzt und merkt jetzt, dass das dieses nicht mehr zur aktuellen Gefahrenlage passt.
Unser Ziel ist es, eine Grundabsicherung zu realisieren. Sollte dennoch ein Angriff erfolgreich sein und eine Infektion mit Ransomware stattfinden, dann sollte nur eine kurze Ausfallzeit auftreten und die Firma nach kurzer Zeit wieder komplett einsatzfähig sein.

1.3 Projektbegründung

Der Schutz der Firma ist die wichtigste Aufgabe. Wenn der Schutz nicht ausreichend ist, kann es ganz schnell zu großen Problemen in der Firma führen, am Ende sogar zur Insolvenz.
Unsere Aufgabe ist, eine kleine Vertriebsfirma mit einer Grundsicherung zu versehen und auch noch dafür zu sorgen das es bei einem erfolgreichen Angriff nur zu einem kurzen Ausfall oder Stillstand der Firma kommt.

1.4 Projektschnittstellen

Für dieses Projekt nutzen wir die vorhandenen Ressourcen, erweitern diese oder wechseln sie aus.
Der Chef hat ein größeres Budget bereitgestellt, um dieses Projekt zu realisieren.
Alle Mitarbeiter werden in dieses Projekt integriert und involviert.
Das Ziel ist klar definiert. Alle möchten lange in dieser Firma noch arbeiten.

1.5 Projektabgrenzung

Dieser Betrieb wurde 2018 im Bereich der Verkabelung und Gebäudetechnik modernisiert. Wir betrachten in diesem Projekt nur den Teil, der noch nicht dem Grundschutz entspricht.

Die vorhandene IT-Infrastruktur ist bereits eine sehr gute Voraussetzung, um den Grundschutz zu realisieren.

Dieses Projekt ist auch wirtschaftlich umsetzbar. Vorhandene Ressourcen werden sinnvoll genutzt und entsprechend modifiziert.

2. Projektplanung

2.1 Projektphasen

Unser gesamtes Projekt läuft vom 25.4.23 bis 23.6.23. Der Projektantrag muss bis 5.5.23 abgegeben werden, Das eigentliche Projekt inkl. Dokumentation ist vom 8.5.23 bis 26.5.23. Nach diesem Termin erfolgt die Erstellung einer Präsentation inkl. Fachgespräche bis 16.6.23. Den Abschluss bilden dann Fachliche Prüfungen und Präsentation.

Zeitplanung 1 Tag = 8 Stunden Verfügbare Zeit = 112 Stunden (bezieht sich auf Phase 2)

Projektphase	**Geplante Zeit**	**verwendete Zeit**
Grundüberblick	3 h	4 h
Planung	8 h	16 h
Netzplan	4 h	3´h
Strukturanalyse	8 h	8 h
Modellierung	4 h	3 h
Neuer Netzplan	4 h	5 h
Umsetzungsplanung Modellierung	8 h	16 h
Berechtigungskonzept	4 h	1 h
Maßnahmenplan	6 h	3 h
Überprüfung, ob Ziel erreicht, wurde	10 h	4 h
Kostenplan	8 h	2 h
IT-Grundschutzcheck	8 h	4 h
Ausblick	2 h	2 h
Dokumentation	32 h	40 h
Pufferzeit	**3 h**	**1 h**

2.2 Probleme während der Projektbearbeitung

Wie bei Anfängern üblich, treten während der Projektbearbeitung Probleme auf, die vorher nicht erkennbar waren. Man überschätzt den Zeitaufwand. Es tauchen Dinge auf, die man beim Projektantrag übersehen und nicht bedacht hat.

Der erste Projektantrag bezog sich auf die Einführung eines ISMS, aber wir haben gemerkt, dass dafür die Zeit, die wir für das Projekt haben, zu kurz ist. Also haben wir das ganze Projekt noch weiter reduziert, so dass es auch zeitlich möglich war. Die Herausforderung war die Backuplösung, die es ermöglichen sollte, innerhalb kurzer Zeit wieder einsatzbereit zu sein.

Die Erstellung der Dokumentation war anfangs auch mit vielen Problemen behaftet. Es ist halt schwierig, die richtigen Worte in der Dokumentation zu finden.

Leider ist das Projekt nur Theorie, weil Praxis fehlt. Somit wissen wir leider nicht, ob sich dieses Projekt genauso umsetzen lässt und vor allem, ob in der Realität vielleicht dann während der Arbeit, nicht doch das eine oder andere Problem auftritt. Aber dafür gibt es ja den ISB, der dann dafür sorgen muss, dass das Sicherheitsniveau immer sehr hoch bleibt.

2.3 Ressourcenplanung

Die notwendigen Ressourcen für diese Projektarbeit sind in diesem 3-Mann-Team jeweils ein Laptop oder PC, die notwendigen Office-Programme für die Dokumentation, Draw.io für die Netzpläne. Die Grafiken wurden selbst erstellt oder je nach Quelle heruntergeladen. Die Aufgaben wurden flexibel geplant. Zuerst haben wir alle Informationen aufgeschrieben und dann gemeinsam sortiert, was benötigt wird. Eine Ideenfindung stand am Anfang des Projektes.
Für den Projektantrag mussten schon Teile des Projektes recherchiert werden, damit der Zeitplan für das Projekt stimmte.

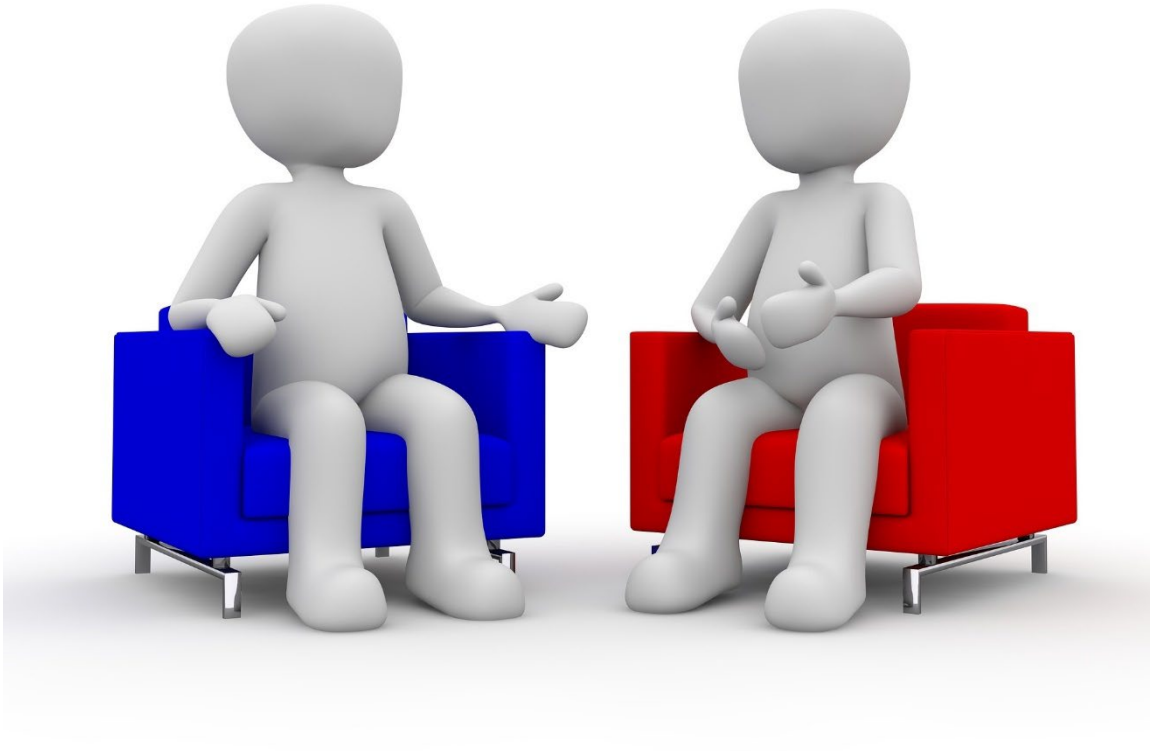
2.4 Überprüfen, ob das Projekt realistisch umgesetzt werden kann

Am Ende unserer Vorbereitungen für dieses Projekt hatten wir bereits den Netzplan Ist und den Netzplan Soll erstellt, der uns einen Überblick gab, was geändert werden muss und wie hoch der Aufwand ist.
Auch die wirtschaftliche Machbarkeit wurde diskutiert und wir kamen zu dem Schluss, dass es wirtschaftlich ist. Wichtig war auch, dass vorhandene Ressourcen einfach anders organisiert wurden und wir damit sogar eine zusätzliche Sicherheit, die Redundanz, geschaffen haben. Die ganzen Maßnahmen in der Umsetzung können auch in einem Zeitrahmen von 3 Wochen durchgeführt werden. Die Maßnahmen, die dann in gewissen Abständen von den Mitarbeitern und IT-Administratoren durchgeführt werden, sind auch geplant, die kann man natürlich nicht als erledigt betrachten, die kommen noch.

Bild erzeugt mit der KI DALL-E

3. Umsetzung des Projektes

3.1 Meeting mit dem Chef



Quelle https://pixabay.com/de/illustrations/besprechung-meeting-gespr%c3%a4ch-1002800/

Der Chef hat die Verantwortung für sein Unternehmen, also fängt die Umsetzung mit einem Meeting an, wo man sich austauscht, welches Sicherheitsniveau der Chef erreichen möchte. Daraus entsteht die Sicherheitsrichtlinie, die die Grundlage für die Firma bildet.

Sicherheitsrichtlinie

Diese Richtlinie gilt ausnahmslos für alle Mitarbeiterinnen und Mitarbeiter bei Aufenthalt in der Firma. Verstöße gegen die Inhalte der Richtlinie können arbeitsrechtliche Konsequenzen nach sich ziehen.

Externer Mitarbeiter werden immer begleitet. Es wird immer darauf geachtet, dass die Sicherheitsvorschriften eingehalten werden.

Es wird auf eine strikte Trennung von Dienstlich und Privat geachtet. So ist die private Nutzung des Internets auf dienstlichen Geräten untersagt. Private Geräte dürfen nicht mit dem Firmennetzwerk verbunden werden und auch nur in Arbeitspausen genutzt werden.

Das Wichtigste für unser Unternehmen ist ein reibungsloser Betrieb, der bei Problemen und Fehlern oder Cyberangriffen schnell wiederhergestellt werden kann. Deshalb hat Cybersicherheit bei uns höchste Priorität.

Unsere Mitarbeiterinnen und Mitarbeiter werden sensibilisiert, damit sie mit den täglichen Gefahren im Bereich der Cybersicherheit umgehen können.

Unsere neue Grundsicherung und die folgenden Maßnahmen sollen uns dabei unterstützen und dafür sorgen, dass sich jeder Mitarbeiter vollkommen auf seine Arbeit konzentrieren kann.

Unser Motto: “Mein Unternehmen, in dem ich arbeite, ist wie mein Zuhause“ Beides möchte man nicht verlieren.

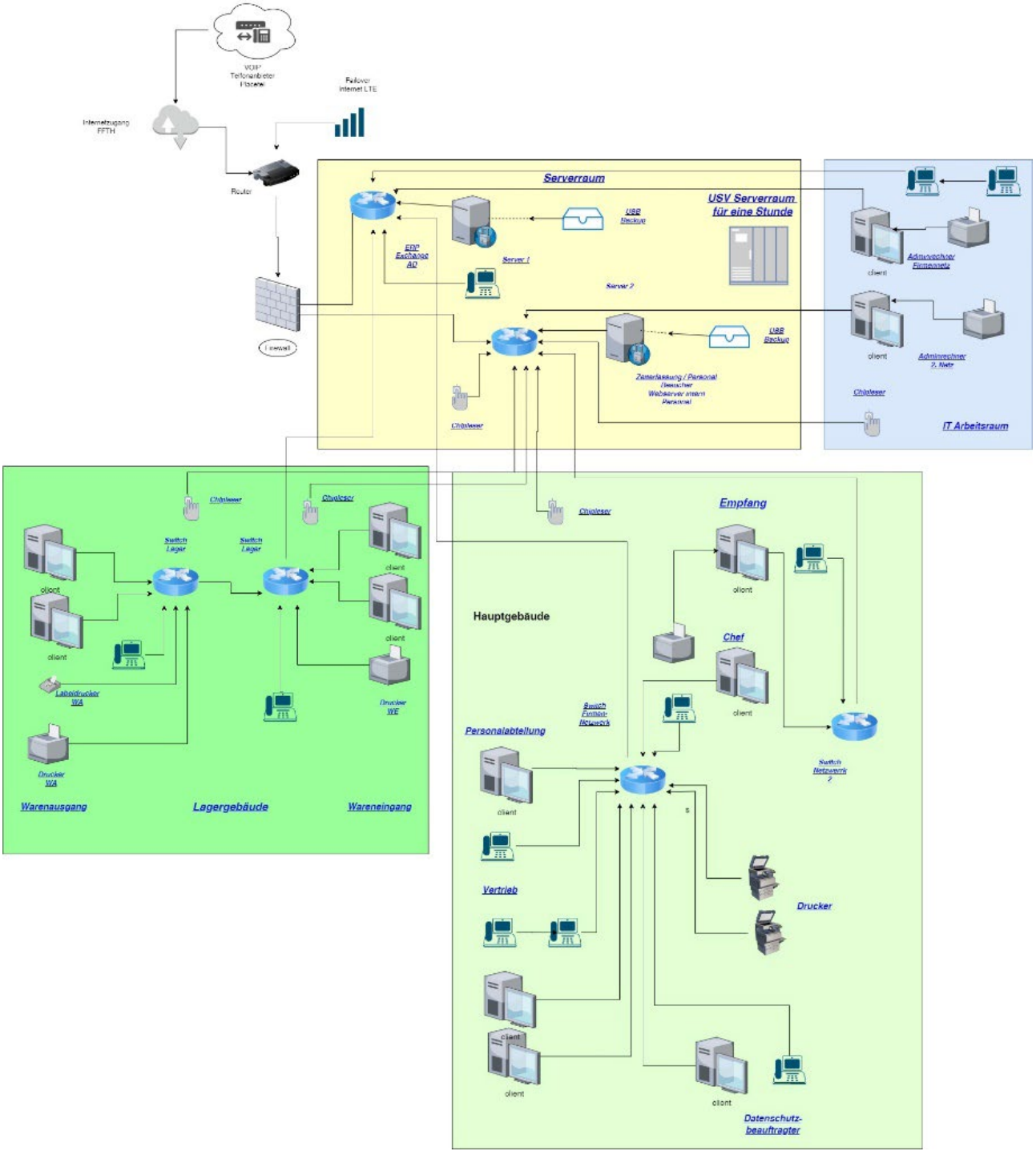
3.2 Netzplan

Der Netzwerkplan steht am Anfang unseres Projekts. Hier haben wir alle IT-Komponenten zusammengefasst und grafisch dargestellt. Die Verbindungen zwischen diesen Komponenten sind auch ersichtlich, sowie auch die räumliche Aufteilung.

Dieser Netzplan hilft uns, das Projekt vernünftig zu starten und ist die Basis für das, was wir wollen. Er ist auch eine sehr gute Grundlage weitere Schritte.

Auf dem Netzplan sieht man, dass versucht wurde, eine gewisse Sicherheit zu realisieren. 2 Server und darauf verteilt die Anwendungen, das Ganze über 2 Netze administriert. Im Büro wurde auch schon der Empfang vom Rest isoliert. Ein Failover Internet zur Sicherheit, nur die 2 Multifunktionsgeräte im Netzwerk, die Drucker größtenteils direkt am PC, die Telefonie über VOIP von einem anderen Anbieter betreut. Alles Dinge, wo die Idee und Umsetzung schon für Sicherheit sorgen sollen. Ein sehr gutes Zutrittssystem mit Berechtigungssystem ist schon vorhanden.

Es wurden aber auch wichtige Dinge übersehen, die zu Problemen führen können. So laufen die Applikationen auf den Servern direkt auf dem Host. Es gibt nur eine Firewall ohne zusätzliche Schutzfunktionen. Auch die Switches sind ohne besondere Sicherheitsvorkehrungen. Auffällig ist auch, dass die Arbeitsplatzrechner alle so aufgestellt sind, dass man leicht und unbemerkt an die hinteren Anschlüsse des Rechners gelangen kann. Was im Serverraum auch auffällt, sind die beiden USB-Festplatten für die Backups, die für alle sichtbar in einem Regal stehen.


Serverraum
USV Serverraum für eine Stunde
IT Arbeitsraum
Hauptgebäude
Empfang
Chef
Personalabteilung
Vertrieb
Drucker
Datenschutz-beauftragter
Warenausgang
Lagergebäude
Wareneingang
Router
Firewall
client

3.3 Strukturanalyse

Der Netzwerkplan ist nun die Voraussetzung für unsere Strukturanalyse. In dieser Analyse haben wir alle Geräte, Arbeitsprozesse, wichtige Arbeitsprozesse, Verbindungen von außen, externe Dienstleister und Gebäude aufgelistet Ein IP-Scan im Netzwerk zeigte uns, welche aktive Geräte im Netzwerk vorhanden sind, der Vergleich mit dem Netzplan zeigt dann sofort ob unberechtigte Geräte im Netzwerk vorhanden sind, oder man einfach Geräte vergessen hat.

Auf dem Netzwerkplan sehr gut zu erkennen, der Versuch eine gewisse Grundsicherheit zu realisieren. 2 Server mit dem Betriebssystem Microsoft Server 2019. Auf einem Server befindet sich die ERP-Anwendung, der Exchange Server und die Windows Active Directory, auf dem anderen Server die Zeiterfassung, das Besuchersystem und das Personalverwaltungsprogramm. Grundsätzlich ist die Verteilung der Anwendungen auf verschiedene Server sehr gut, allerdings waren in unserem Fall alle auf dem Host installiert, was sicherheitstechnisch wieder zu Problemen führen kann. Hätte man Zugriff auf den Host, hätte man auch Zugriff auf die anderen Anwendungen und könnte dort auch den administrativen Zugriff bekommen.

Die getrennte Administration der beiden Server ist eine schlechte Lösung, aber im Endeffekt eher umständlich, da man immer zwischen 2 Rechnern hin und her springen muss. Hier besteht auch schnell die Gefahr, Fehler zu machen, was zusätzliche Sicherheitslücken schaffen kann. Die Telefonie über einen VOIP-Anbieter zu lösen, ist sehr gut, so gibt man die Wartung an spezialisierten Anwender und man muss sich nicht um die Hardware kümmern. Telefon anschließen und es funktioniert. Ports in der Firewall müssen auch nicht geöffnet werden.

Das Backup ausschließlich über USB-Platten ist nur eine Sicherung und kein echtes Backup. Sollte eine Platte defekt gehen, was schnell passieren kann, dann kann man das Backup nicht mehr verwenden. Genauso, ist Ransomware im Netzwerk, dann kann sich diese auch schnell auf das Backup verteilen und somit das Backup wertlos machen. Das Backup ist meistens die letzten Rettungsanker in einem Unternehmen.

Vorbildlich ist die USV-Lösung, die den gesamten Serverraum für 1 Stunde mit Strom versorgen kann. Auch die Switches werden von einer kleinen USV versorgt. Die Clients sind alle mit der Windows Active Directory verbunden und die Daten der Mitarbeiter werden auch in der AD auf dem Server gespeichert, so dass bei einem plötzlichen Ausfall des Clients so gut wie kein Datenverlust entsteht.

Der verwendete Router entspricht den Vorgaben für Business. Er bietet einen Failover Internetzugang. Da man als Failover immer eine andere Technik verwendet als die Hauptinternet, läuft Failover über LTE. Die Firewall ist vom Konzept her gut und effektiv. Es fehlen aber aktuelle Sicherheitsmechanismen, die noch mehr Schutz bieten.

Die Kommunikation mit externen Dienstleistern erfolgt über verschlüsselte E-Mail oder Telefon.

Homeoffice oder mobiles Arbeiten ist in diesem Unternehmen nicht eingerichtet und auch nicht geplant. Dies erleichtert uns die Sicherheitsarbeit.

Das Lager wurde 2018 schon so modernisiert, dass die Vorgaben des BSI alle erfüllt wurden.

3.4 Modellierung

Im Grundschutzkompendium des BSI findet man sehr viele Bausteine, mit entsprechenden Umsetzungshinweisen und das auch für den Grundschutz.
Für unser Projekt sind es im Endeffekt 29 Bausteine, die wir umsetzen.

ORP 1	***Organisation*** Informationssicherheit ist immer eine Gesamtheit von Menschen und Technik betrachten wir komplett. Wer welche Rolle und Verantwortlichkeiten hat und wie diese zusammenspielen und im Falle des eines Problems, wie man dieses Löst.
OPR 2	***Personal*** Die Mitarbeiter in einem Unternehmen sind die, die den Betrieb am Laufen halten. Damit die Mitarbeiter sich aber wirklich nur um Ihre Aufgaben kümmern können, muss das Arbeitsumfeld in Sachen Sicherheit stimmen
ORP 3	***Sensibilisierung*** Die Sensibilisierung der Mitarbeiter ist sehr wichtig in diesem Unternehmen. Erst wenn die Einstellung zur Cybersicherheit stimmt und die Mitarbeiter begriffen haben, warum, erst dann ist die Produktivität gesichert.
ORP 4	***Identitätsmanagement*** Es werden nur die Ressourcen den jeweiligen Mitarbeitern zur Verfügung gestellt, die sie für Ihre Aufgabe benötigen. Nur autorisierte Benutzer dürfen im System arbeiten.
Con 3	***Datensicherungskonzept*** Der letzte Rettungsanker der Firma für die Daten, ist das Backup. Dieses sollte frei von Schadsoftware sein und auch regelmäßig überprüft werden. Professionelle Lösungen bieten dahingehend genau den Schutz, den man braucht und Schutz vor Schadsoftware im Backup auch mit.
OPS 1.1.1	***Allgemeiner IT-Betrieb*** Wir schaffen Voraussetzungen, dass der IT-Betrieb immer ohne Probleme läuft. Das Monitoring, Verwaltung, Dokumentation, Fehlerbeseitigung sowie das Verhalten bei Cyberangriffen sind die Stützpfeiler einer Firma
OPS 1.1.2	***Ordnungsgemäße IT-Administration*** Das Berechtigungskonzept bringt effektiv nichts, wenn man es nicht richtig umsetzt. Auch die richtige Planung der Administration ist dabei sehr wichtig
OPS 1.1.3	***Patch und Änderungsmanagement*** Dieses Management ist die alleinige Aufgabe der It-Abteilung. Es ist eine große Herausforderung, einerseits sollte man schnell Sicherheitslücken schließen, andererseits, könnten dadurch auch neue Probleme oder auch Lücken entstehen
OPS 1.1.4	***Schutz vor Schadprogrammen*** Auch wenn die Anzahl neuer Schadsoftware stetig steigt, so ist es immer wichtig, gegen alles Bekannte geschützt zu sein
OPS 2.2	***Cloudnutzung*** Eine Cloudnutzung ist mittlerweile sehr häufig. Diese ist in unserer Firma aber nicht im Einsatz. Nur für Backuplösungen im Einsatz.
App 1.1	***Office Produkte*** Bei den eingesetzten Office Programmen handelt es sich um die Microsoftprodukte. Dort muss auf richtige Konfiguration geachtet werden, denn schnell entstehen Sicherheitslücken, die man nicht direkt sieht.

App 1.2	***Webbrowsers*** Der Webbrowser ist die Schnittstelle zwischen Rechner und Internet. Eine richtige Konfiguration ist dabei das Wichtigste. Die Benutzung des Internets muss keine direkte Gefahr für unser Firmennetz darstellen.
App 2.2	***Active Directory Services*** Dieses System ist die zentrale Verwaltung der Mitarbeiter und den entsprechenden Berechtigungen. Das muss geschützt werden, denn wer den administrativen Zugang unberechtigterweise hat, kann viel Schaden anrichten.
App 4.2	***ERP-System*** Die Vertriebssoftware ist das wichtigste in unserer Firma, diese wird benötigt, um überhaupt unsere Firma am Laufen zu halten. Deswegen wird das extra betrachtet.
App 5.2	***Microsoft Exchange und Outlook*** Das wichtigste Kommunikationsmittel, für die Firma, aber leider auch das, worüber die meisten erfolgreichen Angriffe erfolgen. Wir betrachten diese Sicherheit extra, um die Risiken für einen erfolgreichen Angriff zu minimieren.
Sys 1.1	***Allgemeine Server*** Server müssen entsprechend geschützt sein, weil die die Voraussetzungen für die Anwendungen bilden
Sys 1.2.3	***Windows Server*** Der häufige Einsatz eines Windows-Server und der damit verbundenen Dienste, erfordert auch eine genaue Betrachtung
Sys 1.5	***Virtualisierung*** Virtualisierung bildet die Grundlage unsere Serversysteme, die sicher sein sollen. Hat einer die Kontrolle über den Virtualisierung-Server, kann er auch auf alle Maschinen zugreifen und Daten unbefugt ändern
Sys 2.1	***Allgemeiner Client*** Die Clients in unserer Firma sollten so sicher konfiguriert werden, dass darüber keine Manipulation möglich ist.
Sys 2.2.3	***Clients unter Windows*** Bei Clients unter Windows ist besonders auf richtige Konfiguration zu achten, da häufig Dienste aktiviert sind, die nicht gebraucht werden.
Sys 4.1	***Drucker, Kopierer und Faxgeräte*** Diese Geräte werden oft unterschätzt, dabei bieten die intern Informationen, die für einen Angriff verwendet werden können
Net 1.1	***Netzarchitektur und -design*** Die gut geplante Netzstruktur bildet die Grundlage für einen sicheren und stabilen Betrieb
Net 1.2	***Netzmanagement*** Das Netzmanagement sollte mit der Informationssicherheit zusammen betrachtet werden. Eine gewisse Grundsicherheit schafft Vertrauen.
Net 3.1	***Router und Switches*** Router und Switche sind die Schnittstellen zu den Mitarbeitern, diese müssen also auch so konfiguriert werden.
Net 3.2	***Firewall*** Die Firewall spielt die wichtigste Rolle bei der Kommunikation zwischen Firmennetz und Internet. Auch intern ist die Rolle groß. Sie regelt auch intern die Zugriffsrechte. Eine falsche Konfiguration kann großen Schaden anrichten

Net 4.2	***VOIP*** Die Kommunikation über Telefon ist in unserer Firma noch sehr oft im Einsatz, deswegen muss das auch richtig konfiguriert sein.
Inf 1	***Allgemeine Gebäude*** Gebäude muss man aus Sicht der Informationssicherheit auch mit betrachten und diese entsprechend optimal schützen
Inf 2	***Rechenzentrum / Serverraum*** Da wir die IT, inklusive Server und Switche in einem Serverraum untergebracht haben, dürfen wir natürlich auch nicht die Vorgaben vergessen
Inf 12	***Verkabelung*** Die Verkabelung sollte auch entsprechend geschützt sein, vor Ausfall, Manipulation und Störung

3.5 Umsetzungsplan der Modellierung

Eine richtige Umsetzungsplanung ist die Voraussetzung für ein hohes Sicherheitsniveau. Der Weg, den wir dabei genutzt haben, wir haben zu jedem Baustein des Grundschutzkompendiums überprüft, ob dieser für unsere Firma Anwendung finden. Dabei waren es am Ende 29 der 111 Bausteine, die wir für die Firma beachten mussten.

Bei dem Festlegen der Maßnahmen spielt eine große Rolle, lässt sich das umsetzen, bringt es für die Sicherheit viel, können die Mitarbeiter auch immer damit umgehen und ist es wirtschaftlich. Wichtig dabei, es nützt nichts, wenn man eine Sache macht und andere unbeachtet lässt. Wir haben versucht, verschieden Fälle durchzuspielen, in Bezug auf Sicherheit.

Der Dreh und Angelpunkt unserer Firma liegt im Backup. Daten sind das, was die Firma braucht, um zu arbeiten. Deshalb ist es umso wichtiger, eine Backuplösung zu realisieren, die auch bei einem Ransomware Angriff zuverlässig die Daten sauber hält und es möglich macht, diese auf unserem System schnell wieder verfügbar zu machen. Der Anbieter Veeam ist genau auf solche Lösungen spezialisiert. Er bietet dahingehend eine komplette Lösung an. Wichtig dabei, wir bekommen eine auf unsere Firma angepasste Lösung, die auch gleichzeitig das Monitoring in unserer Firma übernimmt. Der Anbieter Veeam bietet eine komplette Lösung an, die auch einen sehr guten Schutz gegen Ransomware bietet. Das ist genau das, was unserer Firma braucht, um nur nach einer kurzen Ausfallzeit, schnell wieder einsatzfähig zu sein.

Für die Autorisierung auf Rechnern und Server setzen wir auf eine zusätzliche Methode, die Fido Keys. Diese Hardware-Lösung ermöglicht ein sicheres Einloggen, durch einen zusätzlichen Faktor zum Benutzernamen und Passwort. Das wiederum sorgt dafür, dass es für die Mitarbeiter einfacher ist, weil man sich nicht immer komplizierte Passwörter merken muss. Beim Verlassen des Rechners ist die Abmeldetaste zu betätigen, der Fido Key muss bei Verlassen immer mitgenommen werden. Auch erfolgt eine Abmeldung der Benutzer nach 1 min, wenn keine Aktivität festgestellt werden kann.

Ein ISB wird in der Firma ein fester Bestandteil sein. Seine Aufgaben betreffen den gesamten Bereich der Informationssicherheit. Er führt die Maßnahmen zur Sensibilisierung der Mitarbeiter durch. Er erstellt die Einarbeitungspläne für neue Mitarbeiter und er überprüft in gewissen Abständen, ob die Sicherheitsmaßnahmen noch ausreichend sind, für aktuelle Bedrohungen. Seine Aufgabe auch, immer mal nach neuen Sensibilisierungsmaßnahmen zu schauen.

Sollte externe Dienstleister benötigt werden, so begleitet er diese, oder legt die Vorgehensweise fest, dass die Sicherheit immer gewährleistet ist. Der ISB arbeitet auch aktiv an den Maßnahmen der IT mit. Durch seine umfassende Denkweise ist er dafür ideal, beim Einsatz von was Neuem, auch zu schauen, ob vielleicht schon Sicherheitslücken vorhanden sind, die man vermeiden kann.

Die größte Änderung erfolgt in der IT-Infrastruktur. Die 2 Server bieten ideale Möglichkeiten, um einmal eine Virtuelle Umgebung umzusetzen, sowie durch den 2. Server eine Redundanz und auch gleich die Testmöglichkeit, für Backups zu schaffen. Beide Server werden im Bereich Ram, Festplatte und Netzwerkkarten auf gleiches Niveau erweitert. Sollte ein Server ausfallen, durch technischen Defekt, oder er muss vom Netz genommen werden, wegen eines Cyberangriffs, ist schnell ein Ersatz da, der nur noch mit dem Backup bespielt werden muss, und dann sofort einsatzfähig ist.

Für die Virtualisierung wird die Software Proxmox verwendet. Die Verwaltung dieses virtuellen Systems erfolgt nur vor Ort, wenn man sich am Server direkt befindet. Sollte Support benötigt werden, der vom Hersteller über Fernwartung erfolgt, dann wird diese Möglichkeit explizit freigeschaltet und auch von einem Mitarbeiter der IT begleitet. Diese Möglichkeit der Fernwartung, wird bei Hard und Software grundsätzlich so gemacht. Damit schränke ich schon mal die Angriffsmöglichen ein. Vor allem die Möglichkeiten unbemerkt über einen längeren Zeitraum einen Angriff durch zuführen ist damit eingeschränkt.

Auf dem Proxmox System werden für die Anwendungen jeweils eine eigene virtuelle Maschine erstellt. Damit vermindern wir die Möglichkeiten, für erfolgreiche Angriffe auf das gesamte System. Die Administration der wichtigen sicherheitsrelevanten Sachen wird nur vor Ort zugelassen, im Serverraum direkt. Einerseits bedeutet das, das man für Änderungen direkt am Server sein muss, anderseits, Änderungen erfolgen im laufenden Betrieb eher selten, somit reduziert sich dann der Aufwand, immer vor Ort zu sein. Der wichtigste Aspekt ist aber, dass man eben am Server sein muss, um wichtige Änderungen vorzunehmen.

Das Berechtigungskonzept spielt dabei eine große Rolle. Extrabenutzer für verschiedene Rollen auf dem Server werden eingerichtet, die auch nur einen kleinen Teil administrieren, das hilft auch, die Sicherheit zu erhöhen.

Die bestehende Firewall sowie die Switche werden alle getauscht. Eingesetzt wird jetzt ein System von Ubiquiti mit Firewall und Switchen, was ein optimales Zusammenspiel garantiert.

Wir nehmen eine Segmentierung des Netzes vor, damit eben eine Sicherheit da ist, wenn jemand Zugriff auf das eine Netz hat, nicht auch gleich auf alle anderen Netze Zugriff erlangt. Die Segmentierung wird mit Vlan´s realisiert, wo am Ende auch passende Firewall Regeln eingerichtet werden. Das Ganze bedeutet, dass die Drucker, Telefone jede Abteilung und Administration sich jeweils in einem isolierten Netz befinden. Das Ganze verringert die möglichen Auswirkungen, bei einem Angriff. Weiterhin verringert das auch die Anzahl der Mitarbeiter, über die der Angriff stattfinden kann. Nur Rechner der IT-Abteilung haben noch die Möglichkeit, sich über Fernwartung auf die Clients zu schalten. Dabei muss aber der Mitarbeiter das auch bestätigen. Somit verhindern wir einen unautorisierten Einsatz

Für den Empfangsbereich haben wir was Besonderes vorgesehen. Dort setzen wir ein neues Besuchersystem ein, was aus Rechner mit Monitor, Maus, Tastatur und Drucker besteht und keine Verbindung zum Firmennetz hat. Er dient für alle Aufgaben der Besucher, wie Ausdrucken von Dokumenten. Eingebaut ist das System in einem Schrank, der abgeschlossen ist.

Das Besondere an diesem System, es handelt sich um ein RAM-System. Alle Daten sind nicht auf Festplatte, sondern die ganze Verarbeitung ist nur im Ram. Wenn der Rechner gestartet wird, wird automatisch ein frisches System gestartet. Sollte ein Besucher es also schaffen, einen Virus über USB-Stick auf das System zu bekommen, dann ist dieser Virus für die Zeit des Arbeitens aktiv, kann aber keinem Schaden anrichten, weil dieses System nicht ans Netzwerk angebunden ist. Weiterhin wird dieser Rechner nach jedem Benutzen neu gestartet, so dass dieser Virus auch nicht auf einen anderen USB stick übergreifen kann.

Alle Clients werden durch die Windows Active Directory zentral verwaltet. Die Antiviruslösung auf dem Server schützt automatisch alle Clients. Alle Workstations werden auf Windows 11 Enterprise umgestellt. Dieses wurde schon getestet, dass auch alle Anwender Software Fehlerlos funktioniert. Das Patchen und Updates zu Software, wird auch zentral von der AD gesteuert. Jede Softwareinstallation wird danach richtig konfiguriert, damit Funktionen, die Angriffsmöglichkeiten bieten, einfach nicht da sind. Die Anzahl der installierten Software wird nur auf notwendige Programme begrenzt. z.B. wird zum Surfen nur der Edge verwendet, der auf Sandbox eingestellt ist. Das soll verhindern, das Links, die zu Seiten mit Schadcode führen, nichts anrichten können, weil die in einer Sandbox ausgeführt werden. Eine Cloudnutzung wird im Firmennetz nicht benutzt.

Da viele Angriffe über E-Mails passieren, haben wir uns für E-Mail-Bearbeitung was Sicheres überlegt, was die Möglichkeiten, dass ein erfolgreicher Angriff ausgeführt werden kann, stark einschränkt. Ein Microsoft Exchange-Server ist ja für E-Mail schon vorhanden. Diese Anwendung läuft in einer virtuellen Umgebung. Als Anhänge werden nur PDF-Dateien zugelassen. Diese Anhänge werden überprüft auf Schadsoftware. Microsoft Exchange hat standardmäßig ein Web-Appsystem (OWA) mit dabei. Dieses nutzen wir. Jeder Benutzer, der Emails bearbeitet, loggt sich über den Browser bei seinen Emails ein, das ganze zusätzlich gesichert mit Multifaktor. Da kann jeder seine Emails vernünftig bearbeiten, und auch außerhalb des eigenen Systems und dadurch getrennt von der AD. Wenn Links in Emails enthalten sind, werden diese beim Anklicken in einer Sandbox geöffnet, sowie auch dort weiterbearbeitet. Werden Dokumente über diesen Link heruntergeladen, muss beim Verlassen des Sandbox Browsers darauf geachtet werden, was er genau fragt, was er auf den Rechner kopieren werden soll, was man benötigt. Ein Restrisiko bleibt immer, da die Schnittstelle Mensch eben keine Maschine ist.

Eine sehr wichtige Maßnahme ist, es werden alle Rechner so am Arbeitsplatz platziert, dass ein Besucher nicht mehr so einfach an die Anschlüsse am Rechner kommt, denn bis jetzt ist so, lenkt man den Mitarbeiter ab, kann man ganz einfach, was an den Rechner anstecken, was gefährlich sein kann und Große Schäden verursachen. In dieser Firma werden auch Besucher empfangen und dann zu Besprechungen in den Besprechungsraum durch die Büros geführt. Besucher werden auch nicht unbegleitet durch den Betrieb losgeschickt.

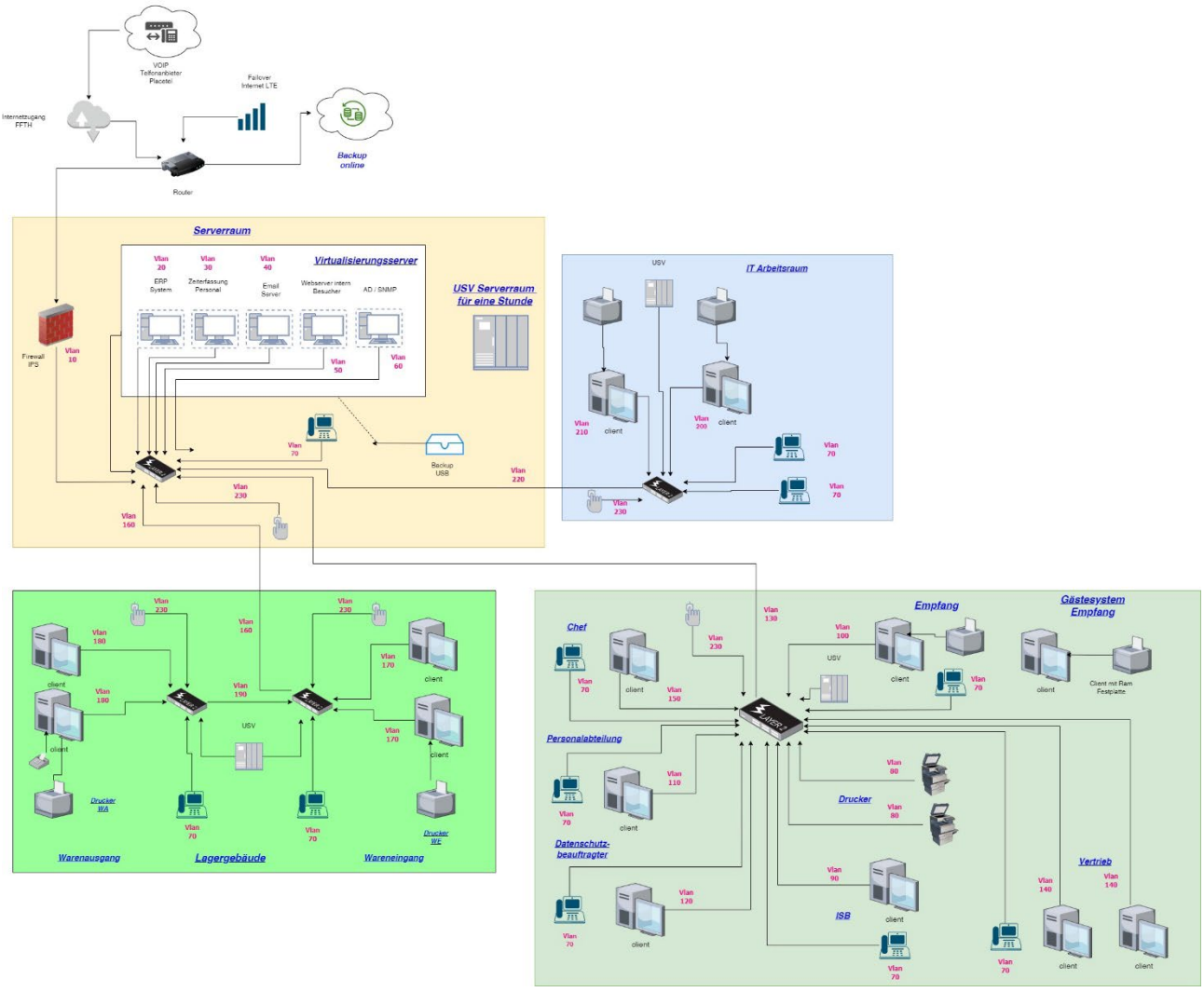
Die Bausteine Inf 1, Inf 2 und Inf 12 wurden 2018 schon bei Neuverkabelung umgesetzt. Dieser entsprechen auch dem BSI-Grundschutzkompendiums.

3.6 Der neue Netzplan für den Soll-Zustand

Aus diesen Maßnahmen, resultiert natürlich jetzt ein neuer Netzplan. Darauf ersichtlich die neuen Strukturen mit Segmentierung.

Auffallend an diesem Netzplan, ist die sehr starke Segmentierung, erkennbar an den eingezeichneten roten Vlan Nummern. Dahinter steckt aber ein sehr gutes Sicherheitskonzept.

Die Firewall spielt dabei eine wichtige Rolle. Wenn man beginnt, das umzusetzen, sollte die Firewall grundsätzlich erst mal die Verbindungen zwischen den Vlan blockieren. Danach kann man ganz genau schauen, wie man die Firewall konfiguriert, welches Netz zu welchem Netz eine Verbindung benötigt, oder ob es ausreicht, wenn man einzelnen IP-adressen nur den Zugriff auf bestimmte Ressourcen in anderen Netzen erlaubt. Man muss beachten, dass man nicht alle Regeln der Firewall auf einmal einrichtet. Sinnvoll ist es, ein Netz komplett zu bearbeiten und die Regeln nach dem Einrichten zu kontrollieren. Nur so erkennt man Fehler in der Konfiguration direkt oder auch Denkfehler.



3.7 Zwischen Fazit

Wir haben erst mal in der Theorie eine sichere Grundbasis geschaffen. Unser Wissen ist leider nur theoretische Kenntnisse. Wir haben verschiedene Angriffsscenarien genommen und auch geschaut, wie sichern wir das. Es wird den 100%tigen Schutz nicht geben, aber diese Lösung sollte zumindest einen sehr großen Schutz bieten.

Wir haben den BSI-Grundschutz entsprechen dem BSI-Grundschutzkompendiums umgesetzt.

Beim BSI-Grundschutz gibt es eigentlich Punkte, die man betrachten sollte. Hier bei unserem Projekt brauchten wir das allerdings nicht, denn der vorhandene Netzplan zeigt ja schon, gewisse Sicherheitslücken. Auch das 2 Angriffsgefährdete Anwendungen nur vorhanden sind, machte es uns einfacher, ein Konzept zu verwirklichen. Wir haben auf die Schutzbedarfsanalyse, den ersten Grundschutz-Check sowie eine extra Risikoanalyse verzichtet.

Was bereits aufgefallen ist, den Lagerbereich haben wir gar nicht betrachtet, bei unserem Projekt. Das mussten wir auch nicht, da der ganze Bereich 2018 nach Vorgaben des BSI umgebaut wurde und auch entsprechend verkabelt. Die Segmentierung und die Konfiguration dieses Bereichs nehmen an den Systemen im IT-Raum vor.

3.8 Berechtigungskonzept

Wenn wir das Netzwerk segmentieren, ist das schon eine gute Sicherheit, aber ohne das richtige Berechtigungskonzept ist es auch nicht die Sicherheit, die wir haben müssen. Schließlich muss man alle Türen schließen, um das Sicherheitsniveau hochzuhalten

Wir haben uns also überlegt, welche Abteilungen müssen, überhaupt Zugriff haben auf welche Anwendung haben und was benötigen Sie dabei für Rechte. Sollte Sie nur lesen können oder auch Schreibrechte haben.

Leserechte sind für Schadsoftware nicht anfällig, da sie nur einen Lesezugriff ermöglichen und damit Dateien nicht verändern können.

Leserechte können aber für weitere Angriffe verwendet werden, wenn man Informationen haben möchte, um den nächsten Angriff erfolgreich durchzuführen.

Wir wählten für das Berechtigungskonzept eine Tabellenform. Diese schafft den schnellen Überblick, wer welche Rechte besitzen sollte.

Nach der genauen Analyse stand dann fest, die Mitarbeiter der IT sind die, die am gefährdetsten sind. Gefolgt von den Mitarbeitern der Personalabteilung und des Vertriebs. Also werden wir am Ende beim IT-Grundschutz-Checks diese explizit betrachten, wie sich Angriffe auswirken könnten.

Besonders bei Mitarbeitern der IT muss man darauf achten, dass die Accounts, die an Ihrem Rechner sind, nur eingeschränkte administrative Tätigkeiten ermöglichen. Genau aus diesem Grund haben wir viele Sachen so eingerichtet, dass man es nur am Server direkt machen kann. In unserem Falle sitzen die Mitarbeiter im Nebenraum, so dass diese Art der Administration keine große Zusatzbelastung darstellt, aber einen enormen Gewinn an Sicherheit

	ERP	Zeit / Perso	E-Mail	Besucher	Windows AD
Chef	nur Leserechte	nur Leserechte	Keine Rechte	Schreib – und Leserechte	nur Leserechte
Empfang	Keine Rechte	Keine Rechte	Keine Rechte	Schreib – und Leserechte	nur Leserechte
Datenschutz	nur Leserechte	nur Leserechte	Schreib – und Leserechte	Schreib – und Leserechte	nur Leserechte
Personal	nur Leserechte	Schreib – und Leserechte	Schreib – und Leserechte	Schreib – und Leserechte	nur Leserechte
Vertrieb	Schreib – und Leserechte	nur Leserechte	Schreib – und Leserechte	Schreib – und Leserechte	nur Leserechte
ISB	nur Leserechte	nur Leserechte	nur Leserechte	Schreib – und Leserechte	nur Leserechte
IT Admins	Schreib – und Leserechte	Schreib – und Leserechte	Schreib – und Leserechte	Schreib – und Leserechte	Schreib – und Leserechte
Wareneingang	nur Leserechte	Keine Rechte	Keine Rechte	Keine Rechte	nur Leserechte
Warenausgang	nur Leserechte	Keine Rechte	Keine Rechte	Keine Rechte	nur Leserechte

Erklärung: **Schreib – und Leserechte** **nur Leserechte** **Keine Rechte**

3.9 Maßnahmenplan für Mitarbeiter und IT

Die Umsetzung des Grundschutzes ist nie ein einmaliges Projekt. Es handelt sich immer um einen Zyklus, der Planung, des Umsetzens der Maßnahmen, der Überprüfung und am Ende der Anpassung

Folgemaßnahmen sind sehr wichtig, für den Erhalt des Schutzniveau in der Firma. Es gibt Maßnahmen für alle Mitarbeiter und nochmals extra für die IT-Abteilung

Folgende Maßnahmen werden für alle eingeführt, die betreffen alle Mitarbeiter und die IT-Abteilung

- Aller 3 Monate erfolgen Schulungen Vor-Ort zum Thema Sicherheit in der Firma
- In den Sensibilisierungsmaßnahmen wird auch gezeigt, wie Betrüger private Informationen verwenden, um an eine Firma zu kommen. Auch wenn man sich mit Ex-Mitarbeiter privat unterhält, sind Themen, die in Verbindung mit der Firma stehen, zu vermeiden.
- Ein monatlicher Newsletter informiert die Mitarbeiter auch über neu auftretende Gefahren
- Beim Anmelden früh werden bei Bedarf Nachrichten gezeigt, und des Desktophintergrund ist angepasst auf Sicherheit
- Da auch Türen vorhanden sind, werden dort auch entsprechende Poster aufgehangen
- Sehr wichtig ist, dass bei ungewöhnlichen Aktivitäten beim Arbeiten diese immer sofort dem ISB oder einem Vorgesetzten zu melden sind.

Folgende Maßnahmen gelten jetzt speziell noch für die Mitarbeiter der IT-Abteilung

- Die Batterien der USV werden täglich auf den Ladezustand kontrolliert, dass dieser voll ist
- Die Lüfter der Geräte im Serverraum werden einmal wöchentlich gereinigt
- Monatlich werden angemeldete Benutzer auf dem Server kontrolliert und mit der Realität abgeglichen
- Die Backuplösung vom Anbieter Veeam bietet eine automatische sichere Überprüfung unserer Backups an, es ist nur darauf zu achten, dass es richtig konfiguriert, ist
- Besondere Maßnahmen treten bei Mitarbeitern in Kraft, die selbst gekündigt haben oder gekündigt wurden. Es gelten dann Bestimmungen, die der ISB in Verbindung mit der IT-Abteilung festlegen.
- Es muss verstärkt darauf geachtet werden, dass die Protokollierung aller Tätigkeiten gewissenhaft durchgeführt wird. Umso genauer und präziser diese Informationen sind, umso besser und schneller geht eine Fehlersuche oder wenn andere Probleme auftreten

3.10 Kostenplan

Wir haben uns entschieden, ein System der Firma Ubiquiti einzusetzen. Das bietet den Vorteil, dass alle notwendigen Sicherheitsfunktionen vorhanden sind, das ganze zentral verwaltet wird und man auch in Zukunft damit weiter Sicherheitsmaßnahmen implementieren kann, wie ein Zugangssystem, Kameraüberwachung

Der Kostenplan bezieht sich ausschließlich auf die Kosten, die für unser Projekt entstehen.

	Einmalige Kosten	Monatliche
Erweitern der Server mit Ram, Festplatten und Netzwerkkarten	5520,- Euro	
Firewall UDM Pro SE inkl. UI Care	665, Euro	
4 mal 24er Switch Ubiquiti inkl. UI Care Enterprise	8392,- Euro	
30-mal Hardware Fido Key 40 Euro	1200,- Euro	
Komplettes System Empfang	1270,- Euro	
Windows 11 Umstellung	0,- Euro	
2-mal Clients Reserve	1600,- Euro	
Backup Lösung Veeam		250,- Euro
Personalkosten 4 x 8 Stunden	960, - Euro	
Komplett	**18547,- Euro**	**250,- Euro**

Damit steht fest, die Kosten für unser Projekt betragen ca. 20000,- Euro einmalig und monatliche zusatzkosten von 250,- Euro. Die Wirtschaftlichkeit unsere s Projektes ist damit sichergestellt.

4.Fazit

4.1 Soll- /Ist-Vergleich

Nachdem wir das Projekt jetzt am Ende angekommen sind, vergleichen wir nochmals den Zustand, den wir am Anfang hatten und den Zustand jetzt 3 Wochen später. Die Sicherheit, gegenüber Cyber-Angriffen ist sehr stark erhöht und sollte uns vor größeren Schäden bewahren. 100% Schutz wird es nie geben. Wichtig ist, dass dieses System in gewissen Abständen überprüft wird, vor allem in Bezug auf neu auftretende Gefahren.

Der jetzt in der Firma eingestellte ISB muss jetzt natürlich dafür sorgen, dass das Sicherheitsniveau in der Firma weiterhin hoch bleibt.

4.2 IT-Grundschutzcheck

Am Ende des Projektes angekommen, ist der IT-Grundschutzcheck. Dabei überprüfen wir, ob alle Punkte, umgesetzt sind und ob es vielleicht noch Sachen gibt, die nicht erfüllt wurden. In unserer Firma waren alle Vorgaben umgesetzt.

Wir haben Angriffe simuliert, dabei gehen wir immer vom schlimmsten Fall aus, ein Mitarbeiter hat auf einen Link geklickt in einer E-Mail, hat dadurch Ransomware aktiviert und diese wird sofort aktiv, oder sie lässt sich Zeit, eh sie aktiv wird.

Bei den ganzen Planspielen haben wir festgestellt, dass die Chance, dass eine Schadsoftware über eine E-Mail aktiviert werden kann, sehr gering ist. Ist dieser Fall mal eingetreten und Schad Software ins System gelangt, können wir schnell reagieren und die Firma auch schnell wieder ans Laufen bekommen. Wir tauschen den Server komplett aus und ersetzen diesen durch den vorhandenen. Damit vermeiden wir auch, dass die Schadsoftware sich noch anderen Stellen, in einem anderen Virtuellen System eingenistet hat. Wir spielen dann nur noch die Backups der einzelnen virtuellen Systeme zurück und sind somit schnell wieder einsatzfähig, da die Konfiguration identisch ist, zum laufenden Server.

Unsere Backuplösung sorgt dafür, dass diese Backups auch sehr gut geschützt sind, dass die Ransomware sich nicht auch da so einfach einnisten kann. Wir erreichen damit also unser Ziel, in wenigen Tagen wieder einsatzfähig zu sein.

Unsere Client System sind ähnlich. Wir haben 2 Ersatzsysteme mit der Grundinstallation da, die bei Bedarf nur noch mit entsprechender Software für den Mitarbeiter bestückt werden müssen.

Vor Ort Versuche, unser Firmennetzwerk mit Schad Software zu verseuchen, sind auch stark eingeschränkt. Besucher haben ein eigenes System, wo kein Zugriff aufs Firmennetz vorhanden ist.

Die Ganzen Clients sind so positioniert, dass man nicht unbemerkt was anstecken kann. Unbenutzte Anschlüsse im Netzwerk sind deaktiviert

Das Ergebnis unseres Grundschutzchecks ergibt, wir haben eine wirtschaftliche Lösung eingeführt, die schon einen sehr guten Schutz bietet und auch für aktuelle Gefahren sehr gut schützt.

4.3. Ausblick

Die Informationssicherheit ist ein Kreislaufprozess, der nie anhält. Es kommen fast täglich neue Gefahren, alte Gefahren tauchen auch wieder auf. Unser System mag im Moment sehr sicher sein, aber auch das kann in gewisser Zeit auch wieder ganz anderes sein.

Wir haben dem ISB hier in der Firma ein System realisiert, was sehr gut ist. Nun liegt es vorzugsweise an Ihm, dass er dieses System in regelmäßigen kürzeren Abständen immer wieder in Bezug auf Sicherheit und aktuelle Gefahren überprüft. Er muss immer mit der Zeit gehen und das System an die aktuellen Gefahrenlage anpassen, oder was ganz Neues einzuführen. Wichtig ist, dass nie aus den Augen zu verlieren. Den wie überall, ein Angreifer schläft auch nicht und nutzt immer neue Methoden.

4.4 Abschluss

Dieses Projekt hat uns gezeigt, wir haben das Wissen, aber uns fehlt die Praxis. Oft in dem Projekt, stellten wir fest, dass wir was vergessen hatten, mit einzubeziehen, Wir haben auch gemerkt, es ist sehr schwer sein würde, selbst in einer kleinen Firma solch ein Projekt allein zu machen. Dazu gehört einfach ein Team. Manchmal rennt man sich fest, dann hilft ein anderer weiter, oder Denkfehler. Der Faktor Zeit war es genauso, man plant einfach zu wenig ein, weil eben doch die Praxis und Berufserfahrung fehlen. Ob dieses Projekt jetzt so in der Realität wirklich funktioniert, werden wir hoffentlich bald jeder selbst feststellen, der die Aufgaben des ISB in einer Firma übernimmt. Vieles hört sich in der Realität sehr gut an, aber kann auch in Der Praxis noch Probleme hervorbringen, weil man eben Sachen vergessen hat, wo man noch nicht wusste, dass es die da auch gibt. Aber eines haben wir ganz deutlich gelernt, es ist immer schwierig, sein Wissen in der Praxis einzusetzen, es stellt immer eine Herausforderung dar. Wir hoffen dar wir nach Abschluss der Ausbildung auch eine passende Arbeitsstelle finden, mit Chefs, die genau das suchen, Mitarbeiter mit frischen und auch außergewöhnlichen Ideen.

Quelle https://pixabay.com/de/illustrations/netzwerk-rund-projekt-plan-1987209/

A.1 Strukturanalyse

Server

Windows Server 2019	Serverraum
Windows Server 2019	Serverraum

Clients

2 x PC Client	IT-Arbeitsraum
2 x PC Client	Büro
1 x PC Client	Empfang
5 x PC Client	Büro
4 x PC Client	Lager

Drucker

5 x Laser	über USB
1 x Label Drucker	über Lan
2 x Kombi Laser	über Netzwerk

Telefone

11 x VOIP	Lan

Switche / Router / Firewall / Chipkartenleser / USB-Platten

1 x LTE-Router	
1x Modem Glasfaser	
1 x Firewall	
6 x Switch	Lan
5 x Chipleser	Lan
2 x Backup USB	

Anwendungen

ERP	Serveranwendung auf Host 1
Microsoft Exchange	Serveranwendung auf Host 1
Internet	geschützt durch eine Firewall hinter Router
IP-Telefonie	ausgelagert zu einen VOIP Anbieter
Zeiterfassung	In Verbindung mit Personalverwaltungssoftware
Personalverwaltung	Serveranwendung auf Host 2
Office Programme	Einsatz auf diversen Clients
Webserver intern	wird benötigt für das Besuchersystem, Anwendung auf Host 2
Active Directory	Serveranwendung auf Host 1, Verwaltung aller IT-Systeme
Backupsoftware	Serveranwendung zur Datensicherung über USB
UPS Versandsoftware	Versandlabel erstellen und Daten an UPS übertragen
LDAP Telefonbuch	Telefonbuch der Telefone mit Schnittstelle zum ERP
virtuelle Maschine	Einsatz für administrative Sachen auf verschiedenen Clients

Gebäude

Hauptgebäude
Büro
Serverraum
Sozialräume
Lager

Arbeitsprozesse

Vertrieb	Auftragsannahme, Auftragsverwaltung, Auftragsabschluß, Supportanfragen, Supportverarbeitung, Supportendverarbeitung, Wareneingang buchen
Empfang	Telefongespräche annehmen und weitervermitteln, Besuchertermine vereinbaren und eintragen, Besucher empfangen und betreuen, Besucher eintragen
Personalabteilung	Zeiterfassung kontrollieren, Gehaltsbearbeitung, Zahlungen anweisen, neue Mitarbeiter erfassen, gekündigte Mitarbeiter löschen
Datenschutz	Datenschutz überprüfen, Sensibilisierungsmaßnahmen
IT-Abteilung	Administration aller Systeme, Patchmanagement, Fernwartung intern, Verwaltung der IT-Infrastruktur, VOIP Administration, Support intern, Betreuung Zeiterfassung, Verwaltung Windows Active
Lager	Wareneingang und Warenausgang, Verpacken, Kommissionieren, Sortieren der Pakete, Verpackungsmaterial verwalten, Lieferschein Bearbeitung

Externe Dienstleister

Software	ERP System
VOIP	Telefonanlage in der Cloud
Versorger	Strom, Wasser
Entsorger	Abwasser, Abfall, Papier, Datenträger
Software	Emailserver Microsoft
Gebäude	Vermieter hat Schlüsselvollmacht
Reinigungskräfte	
Servicetechniker	Systemhaus / Lieferrand Hardware
Internet	Glasfaserzugang Vodafone
Internet LTE	LTE Failover Vodafone
Hardware	Lieferant Hardware IT

Kommunikationsverbindungen

Internet über Glasfaser
Internet Failover LTE
VOIP über Internet

A.2 Umsetzung der Modellierung ausführlich

ORP 1 Organisation

- In der Firma wird ein ISB eingestellt, der für die Informationssicherheit zuständig ist
- Das Konzept, wer welche Aufgaben hat, ist genau festgelegt und spiegelt sich im Berechtigungskonzept wider
- Sollte ein Mitarbeiter Vertretung einer anderen Stelle machen, dann benutzt er dafür auch einen extra angelegten Account mit angepassten Benutzerrechten
- Besucher und Betriebsfremde warten auf Ihren Ansprechpartner beim Empfang und werden immer begleitet
- Sollten Mitarbeiter eine fremde Person im Betrieb feststellen, werden sie diese Person direkt dem Vorgesetzten melden

OPR 2 Personal

- Die Einarbeitung neuer Mitarbeiter, sowie die Regeln, wenn ein Mitarbeiter die Firma verlässt, werden individuell festgelegt. Dabei spielt das Thema Sicherheit eine große Rolle
- Externe Servicedienstleister, unterliegen einer extra Vorschrift, wo die Sicherheit an vorderste Stelle steht
- Jeder externe Dienstleister muss vor Antritt seiner Supportätigkeit bestätigen, dass er alle Hinweise zur Sicherheit gelesen hat und verstanden.
- Es wird immer versucht, dass die Mitarbeiter auch durch Schulungen so qualifiziert sind, dass sie gefahrlos arbeiten können und Fehler vermieden, werden
-

ORP 3 Sensibilisierung

- Aller 3 Monate findet eine Vor-Ort-Schulung zur Informationssicherheit statt
- Jeden Monat gibt es einen Newsletter mit Informationen
- Es werden Desktop Themen verwendet, die dezent auf das Thema hinweisen
- An der Tür gibt es Poster auch mit Infos
- Die Mitarbeiter werden in die Benutzung der Hardware eingewiesen. Sollte es Probleme geben, meldet sich der Mitarbeiter sofort, eh er anfängt zu probieren

ORP 4 Identitätsmanagement

- Benutzerrechte werden anhand der Tätigkeit festgelegt, heißt bei Vertretungen, werden auch extra Benutzer verwendet, damit die Vertretung die Tätig richtig durchführen kann.
- Es werden alle originalen Gast Konten und Administratorkonten deaktiviert
- Die Protokollierung ist Bestandteil der Admins und beinhalt alles, was gemacht wurde
- Die Zugangskontrolle zu den Räumen ist durch ein Chipsystem gewährleistet und dabei ist genau festgelegt, wer welche Türen benutzen, darf. Sollte ein Mitarbeiter mal in einen für Ihn nicht zugänglichen Bereich, wird er von einem Mitarbeiter aus dieser Abteilung abgeholt
- Sollte Passwörter benötigt werden, dann wird sich mit der IT abgestimmt, wie diese gespeichert werden. Ansonsten nutzen wir Fido Keys, was Passwortlos funktioniert
- Zu dem Benutzen eines Systems ist der Fido Key zu verwenden

Con 3 Datensicherungskonzept

- Das Thema Backups ist sehr wichtig, denn auch im Falle, dass das System durch Schad Software befallen ist, müssen die Backups immer noch einsatzfähig sein.
- Als Backupsoftware setzen wir Veeam Essentials ein. Diese bietet höchste Sicherheit auch für den Fall, das ein erfolgreicher Angriff mit Ransomware erfolgte.
- Aufgrund der Reverenzen und des erfolgreichen Konzeptes, haben wir uns für diese Lösung entschieden.
- Der Test der Backups erfolgt in regelmäßigen Abständen auf dem 2. Server, der zur Redundanz dient. Damit ist sichergestellt, das gefahrlos getestet werden kann.
- Bei dem Anbieter Veeam handelt es sich um einem Professionellen Anbieter, der schon länger auf dem Markt ist und sich ausschließlich um Backuplösungen kümmert. Dadurch sind Ihm alle möglichen Anforderungen bestens bekannt und werden auch erfüllt.

OPS 1.1.1 allgemeiner IT-Betrieb

- Die Aufgaben der IT-Abteilung betreffen erst mal alle Anfragen und Probleme der Mitarbeiter
- Sollte man feststellen, dass man Probleme bei Software nicht lösen kann, wird sich mit dem Support der Softwarefirma in Verbindung gesetzt, so dass es eine schnelle Problemlösung gibt
- Probleme bei Arbeiten werden direkt dem ISB oder einem anderen Verantwortlichen gemeldet
- Es besteht eine Möglichkeit, betriebsintern via Remote Desktop, auf den Mitarbeit Client zuzugreifen, um das Problem zu lösen oder dann doch vor Ort das zu machen. Um das zu nutzen, muss der Mitarbeiter am Arbeitsplatz zustimmen.
- Das Wichtigste in der Firma, ist das richtige Berechtigungskonzept. Es soll sicherstellen, dass im Falle eines Falles der Schaden begrenzt, bleibt

OPS 1.1.2 Ordnungsgemäße IT Admin

- Das Vertretungsmanagement für IT-Admins ist sehr gut geregelt, selbst bei Ausfällen von den 3 eigenen Mitarbeitern ist die Vertretung geregelt, durch Ersatz von einem Systemhaus
- Sollte ein Mitarbeiter der IT den Betrieb verlassen, gelten besondere Vorschriften, diese werden schriftlich bestätigt und der Mitarbeiter bekommt das ausgehändigt. So gilt Schweigepflicht, dann werden die Passwörter alle gewechselt, wenn dieser Mitarbeiter den Betrieb verlassen hat. Auch werden alle Mitarbeiter informiert, dass dieser Admin nicht mehr für die Firma im Einsatz ist.
- Die Mitarbeiter sollten auch privat darauf achten., bei Kontakt mit diesem ehemaligen Mitarbeiter, das Fragen zur Firma tabu sind.
- Er werden die Dokumente des ehemaligen Mitarbeiters geprüft, wo er was administriert hat, ob dort Sachen gemacht wurden, die nicht zu der Aufgabe zählte.
- Ganz wichtig ist, dass alles sehr schnell nach dem Verlassen des Mitarbeiters passiert, vor allem wenn er den Betrieb verlassen musste, von der Geschäftsführung aus
- Es findet eine Protokollierung aller administrativen Vorgänge statt, dabei wird genau dokumentiert, wann was gemacht wurde, was genau geändert wurde und wer die Änderungen vorgenommen hat und vor allem warum das gemacht wurde.
- Die Protokollierung wird extra verwaltet.
- Für die Administration der einzelnen virtuellen Systeme, werden extra Benutzer angelegt, die nur den Zugriff auf dieses System explizit haben
- Administratoren arbeiten mit einem Standardbenutzer, ohne Adminrechte

OPS 1.1.3 Patch und Änderungsmanagement

- Patche werden zuerst auf einem unabhängigen System getestet, in einer isolierten Umgebung
- Erst wenn das als ok eingestuft ist, werden diese an alle Clients verteilt
- Patche werden meist gesammelt und dann auf einmal eingespielt, davor wurde ein Sicherungspunkt auf den Clients erstellt. Ausgenommen davon sind wichtige Sicherheitspatche.
- Nach dem Patchen werden alle Einstellungen kontrolliert, in Bezug auf Sicherheit
- Zuständig für Patches und Konfiguration der Clients und Server ist nur allein die IT-Abteilung
- Beim Administrieren wird ein Extra-Account benutzt, der Adminrechte hat, aber Rechte, die nicht benötigt werden, sind nicht vergeben
- Bei Anwendungsprogrammen ist immer die neueste Version zu verwenden, die getestet vom Hersteller und freigegeben wurde. Es dürfen keine Beta oder sonstige Versionen verwendet werden

OPS 1.1.4 Schutz vor Schadprogrammen

- Wir verwenden ein mehrstufiges Sicherheitssystem aus einer Lösung einer NextGen Firewalls, Switchen und End Point Security als zentrales Element auch für alle Clients
- Die Virendefinitionen werden zentral auf alle Clients verteilt
- Alle Mitarbeiter sind angewiesen, sollten Virenwarnungen auftauchen, sich bei der IT-Abteilung direkt zu melden, dass die Meldungen analysiert werden können und mögliche Ursachen behoben, werden

OPS 2.2 Cloudnutzung

- Die Cloudnutzung ist begrenzt auf die Backuplösung. Diese läuft unabhängig vom produktiven System.

App 1.1 Office Produkte

- Es werden keine Office Dokument von außen akzeptiert. Diese werden alle gesperrt. Nur das Format PDF ist erlaubt
- In den Office Programmen selbst sind Skripte und sonstige, was einen Schadcode enthalten könnte, nicht aktiv
- Das der Browser Edge schon viele Sachen öffnen kann, auch Office Dokumente, wird der bei der ersten Ansicht genutzt. Dabei läuft der Browser in einer Sandboxumgebung. Das Ganze bezieht sich auf Dokumente, die im laufenden Betrieb geöffnet werden müssen und die nicht aus E-Mails stammen. Dokumente oder Links aus Emails werden gesondert behandelt.
- In Schulungen und Newslettern sollte man immer auf Gefahren durch externe Dokumente darauf hinweisen und auch Gefahren zeigen
- Dokument, die die Notwendigkeit haben, sicher übermittelt zu werden, werden extra geschützt vor dem Versand

App 1.2 Webbrowsers

- Auf Clients wird nur der Browser Edge eingesetzt, in der neuesten Version. Aktiviert im Browser selbst, sind nur Funktionen, die nicht für Schadcode genutzt werden können
- Der Browser wird im normalen Betrieb auch im Sandboxmodus genutzt, was eine gewisse Sicherheit bietet
- Der Browser unterstützt auch alle aktuellen Verfahren zur Sicherheit beim Internet surfen
- Wo es geht und intern notwendig ist, werden Zertifikate verwendet, bei Zugriff auf Programme und Funktionen
- Für das Einloggen auf Webseiten werden alle verfügbaren Sicherheiten verwendet. Dabei werden Passwörter mit einer Mindestlänge von 16 Stellen verwendet, generiert durch einen Zufall Generator am PC
- Wichtig ist, dass der Browser mit allen verfügbaren Sicherheiten so konfiguriert ist, dass man sicher ist, aber auch das Internet nutzen kann

App 2.2 Active Directory Services

- Über die Windows Active Directory werden die Clients konfiguriert, wie z.b. Nachrichten, Deaktivierung von USB-Ports, Desktophintergründen
- Die Clients werden alle auf das richtige Berechtigungskonzept getestet, das auch kein Fehler vorhanden ist
- Das administrative Berechtigung ist so aufgebaut, dass man Aufgaben verteilt, und damit verhindert, dass nicht einer, alles ändern kann
- Die verwendeten Gruppenrichtlinien werden genau geplant und dann nacheinander umgesetzt, für jeden Mitarbeiter einzeln und danach auch direkt getestet, ob diese stimmen
- Viele wichtige Services können nur Lokal vor Ort gemacht werden, so dass man im Serverraum sein muss
- Für Notfallkonten werden extra langem und kompliziertem Passworte verwendet und diese werden aufbewahrt in einem Banksafe
- Die Administration der Windows Active Directory ist nur auf 2 Konten beschränkt, wo man auf richtige Sicherheitseinstellungen achtet

App 4.2 ERP-System

- Da das ERP-System unsere Firma am Laufen hält, wird dort besonders auf richtige Konfiguration geachtet. Nur wer unbedingt in dem System arbeiten muss, bekommt Schreibrechte
- Das ERP-System läuft auf einer eigenen Virtuellen Maschine
- Der Zugriff von Extern (für den Support) wird explizit freigeschaltet, und beim Zugriff wird das ganz begleitet von einem Mitarbeiter der IT

App 5.2 Microsoft Exchange und Outlook

- Der Microsoft Exchange-Server läuft auf einer eigenen virtuellen Instanz
- Zur E-Mail-Abfrage wird das OWA-System vom Exchange-Server genutzt
- Das Einloggen in die E-Mails erfolgt über den Browser mit einer zusätzlichen Authentifikation
- E-Mails werden komplett im OWA-System bearbeitet
- Öffnen von Links oder Dokumenten erfolgt im Sandbox-System Edge
- Anhänge werden alle gesperrt, bis auf PDF
- Die Sicherung des Exchange-Servers erfolgt im Backup-Konzept

Sys 1.1 Allgemeine Server

- Der Server befindet sich in einem abschließbaren Serverschrank. Alle anderen Notwendigen Komponenten sind auch in diesem Untergebracht.
- Die Administration erfolgt bei vielen Grundsätzlichen Anwendungen nur Lokal vor Ort
- Der Zugang zum Serverraum ist geschützt durch ein Zugangssystem, das mittels Chips funktioniert
- Für die Anmeldung am Server selbst wird Multifaktor Autorisierung mit Fido Key verwendet. Nur Administratoren der IT haben diesen. Ein Ersatz Fido Key liegt, wie auch die Passwörter zu den Notfallkonten, in einem Banksafe
- Alle Schnittstellen, die nicht verwendet werden, werden gesperrt
- Bei der Einrichtung des Servers werden nur Dienste aktiviert, die Explizit für den Betrieb nötig sind
- Bei der Erstinstallation werden alle Veränderungen dokumentiert, so dass man nachträglich bei Problemen auch mögliche Fehler findet.
- Es wird kontrolliert, dass die Protokollierung auf dem Server vollständig aktiviert ist und auch alle Vorgänge aktiv sind.
- Sollte der Server neu gestartet werden, so ist darauf zu achten, dass der richtige Grund für diesen Neustart ausgewählt wird.
- Da wir von 2 Servern auf einen umgestiegen sind, haben wir dann 2 identische Server, wo damit sogar eine Redundanz vorhanden ist. Somit ist eine schnelle Wiederverfügbarkeit gegeben, bei Ausfall oder einem Cyber-Angriff. Es kann auch eine gefahrlose Prüfung von Backups erfolgen.

Sys 1.2.3 Windows Server

- Eingesetzt wird ein Server 2019, der vorhanden ist
- Die passende Lizensierung wird angepasst
- Clouddienste werden nicht genutzt und deaktiviert
- Wir nutzen ein eine Virtuelle Umgebung. Darauf installiert jeweils ein einzelner Server für eine Anwendung. Für welche Anwendung es möglich ist, installieren wir die Server Core Version. Diese vermindert die Angriffsfläche des Servers nochmals.
- Jegliches nach Hause Telefonieren des Servers wird unterbunden, vorzugsweise auf dem Server selbst und wenn das nicht möglich sein sollte, in der Firewall

Sys 1.5 Virtualisierung

- Wir benutzen Proxmox VE als Virtualisierungslösung
- Die Administration findet ausschließlich lokal vor Ort statt
- Wenn der Support des Herstellers genutzt werden muss, wird dafür extra eine Verbindung erstellt, die nach Gebrauch, sofort deaktiviert wird
- Diese Virtuelle Server liegt gespiegelt auf einem anderen Sever, so dass eine Redundanz gegeben ist für einen schnellen Wiedereinsatz nach Problemen
- Für die Virtualisierung werden die bestehenden Server entsprechend aufgerüstet. Wichtig dabei, dass genügend Netzwerkkarten vorhanden sind, damit die Netztrennung auch richtig wirksam ist und die Konfiguration sauber eingestellt werden kann.
- Die Performance des Virtuellen Servers wir immer kontrolliert und getestet, damit genug Ressourcen auf Abruf vorhanden sind
- Die Zeitsynchronisation liegt zentral im Netzwerk

Sys 2.1 Allgemeiner Client

- Es wird zur Anmeldung am Clientsystem eine Autorisierung mittels Fido Key genutzt. Dieser wird auch benötigt, wenn man den Arbeitsplatz verlassen hat, um sich wieder anzumelden
- Mitarbeiter müssen beim Verlassen des Arbeitsplatzes die Abmeldetaste drücken
- Eine automatische Abmeldung des Systems wird nach 1 min unbenutzt eingeleitet
- Jegliche Einstellungen und Patches werden zentral vom Server verwaltet
- Die Verwaltung des Schutzprogramms gegen Schadsoftware wird auch vom Server verwaltet
- Die Einstellung des Bios und des Bootvorgangs wird auf sicher eingestellt, dass keine Manipulation direkt möglich ist
- Die Nutzung von Cloudfunktionen ist deaktiviert und auch nicht nötig
- Die Clients werden so am Arbeitsplatz positioniert, dass sie für Besucher nicht erreichbar sind

Sys 2.2.3 Clients unter Windows

- Auf den Clients wird überall Windows 11 Enterprise installiert und verwendet
- Die Installation wird nach der Neuinstallation überprüft, es werden unnötige Sachen entfernt, oder deaktiviert
- Es werden nur Konten in der AD verwendet
- Jeder Mitarbeite auf einem Client arbeitet nur mit Benutzerrechten

Sys 4.1 Drucker, Kopierer und Faxgeräte

- Im Netzwerk sind nur 2 Kombigeräte, die restlichen Drucker sind nur per USB am Rechner verbunden
- Die Konfiguration erfolgt über gesicherte Verbindung zum Drucker
- Der Drucker selbst speichert nur wenn nötig für den Druckvorgang und dann auch nur verschlüsselt
- Am Empfang wird ein Extrasystem für Gäste vorhanden sein, was keine Netzwerkverbindung hat und was nach jedem Benutzen neu gestartet wird
- Die Löschung interner Druckerdaten erfolgt täglich
- Die Drucker werden so aufgestellt, dass sie nicht direkt verrückt werden können und zusätzlich werden diese noch gesichert, über ein Sicherungsseil an der Wand
- Die Wartung und Reparatur der Geräte erfolgt durch einen zertifizierten Serviceanbieter. Mit diesem wurden Randbedingen für die Sicherheit vereinbart, die auch unterschrieben wurden
- Fehldrucke oder Blätter, die nicht mehr gebraucht werden, werden gesondert entsorgt. Dafür nutzen wir einen speziellen Schredder

Net 1.1 Netzarchitektur und –design

- Die Netzstruktur wird über Segmentierung gelöst, dafür verwenden wir passende Geräte, die unsere Anforderungen erfüllen.
- Es wird eine Dokumentation erstellt, die erst mal einen Netzplan enthält und auch einen Plan, wo welche Dosen verbaut wurden und Anschlüsse vorhanden sind
- Unbenutzte Netzwerksdosen werden deaktiviert und nur auf besondere Anforderung freigegeben
- Diese Unterlagen werden in einem Safe als gedruckte Dokumentation aufbewahrt
- Der Netzplan und Verkabelungsplan werden halbjährlich kontrolliert, Änderungen werden so bald erfolgt, direkt in den Netzplan übernommen

- Die Segmentierung bildet eine wichtige Grundlage der Sicherheit, gesteuert durch die Firewall
- Als Firewalls werden Enterprise Produkte eingesetzt. Diese beinhalten alle Voraussetzungen.
- Um die Netzstruktur Sicher zu halten und auf mögliche Änderungen vorbereitet zu sein, werden passende Netzwerk-Komponenten eines Herstellers genommen, da diese ein optimales sicheres Zusammenspiel bieten
- Die Firewalls stellen die sicheren Umgebungen zur Verfügung, intern wie auch extern und bieten dadurch auch die richtige Segmentierung für wichtige Bereiche

Net 1.2 Netzmanagement

- Die ganze Planung für die neue Netzwerkstruktur ist bereits erfolgt und es existiert auch ein neuer Netzplan, wo die Segmentierung auch sichtbar ist (Vlans)
- Die Netzwerkkonfiguration wird nach jeder Änderung direkt gesichert, heißt, von jedem Switch und Firewall
- Damit die Protokolldatei in der Zeit immer stimmt, wird im gesamten Netzwerk eine zentrale Zeitsynchronisation verwendet
- Die Überwachung der Netzwerkkomponennten erfolgt durch unsere Komplettlösung von Veeam.

Net 3.1 Router und Switches

- Es werden nur Geräte im Netzwerk eingesetzt die ein auch alle Funktionen beinhalten und auch ein gutes Zusammenspiel haben
- Die Produktserie von Ubiquit hat den Vorteil, dass man sie zentral verwaltet, somit schnell Fehler erkennen kann und beheben kann und vor allem das man die Segmentierung sehr genau vornehmen kann.
- Die Administration der Komponenten erfolgt vorzugsweise lokal vor Ort
- Da administrative Eingriffe immer dokumentiert werden, sind diese Tätigkeiten auch mit dokumentiert
-

Net 3.2 Firewall

- Wir verwenden 1 Firewall und segmentieren das komplette Netzwerk
- Es wird auf eine sorgfältige Konfiguration geachtet und nur Notwendige Ports geöffnet
- Sollte das IPS melden, das, was blockiert wurde, wird dieser Meldung direkt nachgegangen, um sie zu analysieren und bei Bedarf neue Schutzmaßnahmen einzusetzen
- Der Zugang zur Administration wird mit den Möglichkeiten, die vorhanden sind, gesichert
- Die Administration der Firewall kann nur intern und vor Ort erfolgen
- Wir verwenden ein IPS / IDS System in der Firewall

Net 4.2 VOIP

- Die VOIP Telefonie wird über einen Anbieter abgewickelt, wo man sich im Browser sicher einloggt und die Anlage konfiguriert

Inf 1 Allgemeine Gebäude

- Im Zuge der Revision 2018 wurden die Anforderungen aus dem Grundschutzkompendiums schon umgesetzt

Inf 2 Rechenzentrum / Serverraum

- Im Zuge der Revision 2018 wurden die Anforderungen aus dem Grundschutzkompendiums schon umgesetzt

Inf 12 Verkabelung

- Im Zuge der Revision 2018 wurden die Anforderungen aus dem Grundschutzkompendiums schon umgesetzt

A.3 Quellennachweise

BSI-Grundschutzkompendium

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

Bilder Erzeugung mit Dall-E

https://labs.openai.com/

Diagramme mit Draw.io

https://app.diagrams.net/

Bilder

https://pixabay.com/de/