Landesamt für Sicherheit in der Informationstechnik

LSI-Leitfaden

Ransomware

Stand: 22.08.2023
Version: 1.2

Landesamt für Sicherheit in der Informationstechnik
Keßlerstraße 1
90489 Nürnberg
beratung-kritis@lsi.bayern.de
Telefon: 0911 21549-525

Vorwort

Es existieren unterschiedliche Arten von Schadsoftware (engl. Malware). Je nachdem, welchen Zweck und welche Zielsetzung diese Angriffssoftware hat und wie sie sich ausbreitet, wird sie unter anderem eingeteilt in Würmer, Trojaner, Viren, Spyware, Scareware, Adware oder Ransomware. In der letzten Zeit nahmen die bekannt gewordenen Fälle von Verschlüsselungen mit Ransomware stark zu.

Bei einer Infektion mit Ransomware werden die Daten des Geschädigten verschlüsselt, sodass diese nicht mehr genutzt werden können. Anschließend wird der Geschädigte von den Tätern erpresst. Denn um die Daten wiederherzustellen, braucht es einen Schlüssel, welcher gegen Lösegeld (engl. Ransom), meist in Form einer Kryptowährung wie z.B. Bitcoins, erworben werden kann. Ransomware hat sich inzwischen zu einem lukrativen Geschäftsmodell für Kriminelle entwickelt. Zu den bekanntesten Angriffen mit Ransomware gehören:

Oiltanking	Kaseya	Anhalt-Bitterfeld
Beim Angriff auf das Tanklogistikunternehmen kam es zu Einschränkungen an 13 Be- und Entladesystemen der Tanklager von „Oiltanking“. Tanklastwägen konnten nicht mehr befüllt werden.	Durch ein manipuliertes Update erhielten ca. 60 deutsche Kunden (die meisten auch IT-Dienstleister) einen Erpressungstrojaner. Bedingt durch die Vielfältigkeit der Kunden waren weltweit ca. 1500 Unternehmen betroffen.	Im Landkreis Anhalt-Bitterfeld war selbst mehrere Monate nach dem Cyberangriff im Juli 2021 kein regulärer Betrieb möglich. Der Katastrophenfall wurde ausgerufen.

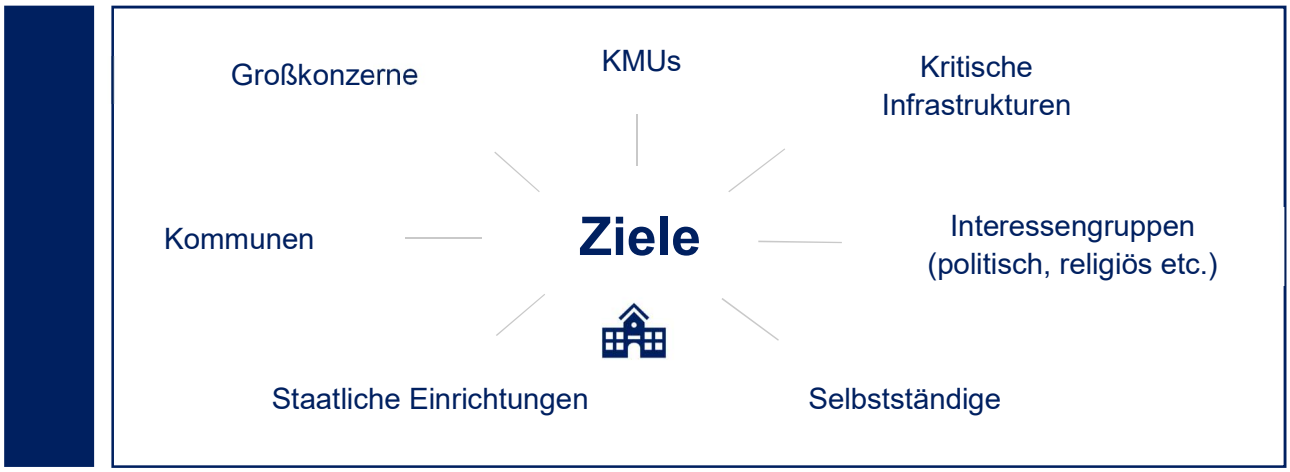
Wie die genannten Fälle zeigen, können Angriffe mit Ransomware weitreichende Konsequenzen für die Betroffenen und deren Kunden nach sich ziehen. Inzwischen sind die Kriminellen nicht nur auf die Verschlüsselung der Systeme und das damit verbundene Lösegeld aus. Oft laden sie zusätzlich noch Unternehmensdaten herunter und drohen mit einer Veröffentlichung dieser.

Ziel dieses Leitfadens ist es, Sie bei der Umsetzung von vorbeugenden Maßnahmen zu unterstützen, um ihre Organisation vor Ransomware zu schützen sowie die möglichen Auswirkungen eines Ransomware-Angriffs abzuschwächen.

Im Nachfolgenden wird beschrieben, welche Ziele Ransomware-Angreifer haben und wie ein Angriff typischerweise abläuft. Da niemand vor einem Ransomware-Angriff absolut sicher sein kann, wird darauf eingegangen, wie man eine Infektion erkennen kann und was man tun sollte, sobald die Organisation mit Ransomware infiziert wurde. Der folgende Abschnitt beschreibt, wie man sich und seine Organisation bestmöglich vor Angriffen schützen kann und enthält Tipps, welche Maßnahmen man treffen kann, um – falls doch eine Verschlüsselung aufgrund neuartiger Angriffstechniken nicht vermieden werden konnte – dennoch bestmöglich auf eine Wiederherstellung vorbereitet zu sein.

Ransomware kann jeden treffen. Cyber-Kriminelle versuchen, in der Breite leicht angreifbare Ziele über bestehende Sicherheitsmängel zu kompromittieren. Dabei nutzen sie oft das Angebot anderer Cyber-Krimineller, welche Ransomware als einkaufbare Dienstleistung (Ransomware-as-a-Service = RaaS) anbieten.

Einerseits streuen die Cyberkriminellen ihre Angriffe dabei oft ungezielt in die Breite, andererseits gibt es auch zielgerichtete Angriffe. Zielgerichtete Angriffe richten sich besonders gegen Organisationen, die wertvolle Informationen besitzen oder besonders zahlungsfähig erscheinen. Weitere Kriterien können eine besondere Bedeutung für das Gemeinwesen (kritische Infrastruktur) oder ein besonderer, politischer Fokus sein. Sicherheitsmängel wie etwa nicht aktuell gepatchte IT-Systeme, Unterbesetzung oder mangelnde Ausbildung des IT-Sicherheits- und Gesamtpersonals sowie unzureichend gesicherte, externe Schnittstellen erleichtern Angreifern das Eindringen in die Organisationsnetzwerke.
Erschwerend hinzu kommen Amateure, die sich wahllos an leicht erreichbaren Systemen ausprobieren möchten, gepaart mit regelmäßig neu entdeckten (Zero-Day-) Schwachstellen.



Das folgende Kapitel beschreibt den Ablauf eines Angriffs mit Ransomware.

Phase der Aufklärung

Angreifer sammeln Informationen über potentielle Ziele:

- Viele der relevanten Informationen sind bereits legal über Unternehmenswebseiten oder andere öffentlich zugängliche Seiten einsehbar. Es können aber auch erste, verdeckte Scans beim potentiellen Ziel erfolgen.
- Kriterien der Angreifer: geringe Komplexität des Angriffs, Wert der Unternehmensdaten und das finanzielle Potential des Unternehmens (erzielbare Lösegeldsumme).

Phase des Eindringens

Angreifer verschaffen sich Zugang:

- Angriffsvektoren: Phishing, E-Mail, infizierte Speichermedien etc. (diese Beispiele zielen vor allem auf den Faktor Mensch als Schwachstelle ab).
- Weitere Angriffsvektoren: Drive-by-Downloads, Brute-Force-Angriffe, Passwort-Guessing, gezieltes Ausnutzen ermittelter Schwachstellen in IT-Systemen z.B. durch eine veraltete Version (sobald eine Schwachstelle ermittelt ist, kann oft direkt auf ein vorgefertigtes Exploit-Kit aus dem Darkweb zurückgegriffen werden).
- Bereits in dieser Phase wird oft Schadcode (sog. Backdoor) platziert, um sich später wieder mit dem System verbinden und den Angriff ausweiten zu können.

Phase des „lateral movement“

Angreifer bewegen sich möglichst unbemerkt durch das interne Netz und suchen nach wertvollen Informationen und Dateien, hierbei werden auch weitere Angriffsziele identifiziert und kompromittiert.

Phase der Rechteausweitung

Angreifer versuchen, ihre Handlungsmöglichkeiten zu erweitern und an weitere Systemrechte zu gelangen.

- Unter Umständen wiederholt sich dann mehrfach die Phase des „lateral movement“ jeweils mit erhöhten Rechten.

Phase des Abgreifens von Daten

- Mit Drohung der Veröffentlichung von abgegriffenen Daten wird oft versucht den Druck auf die Geschädigten zu erhöhen.

Phase der Verschlüsselung

- Ransomware ist heutzutage ein eigenes Geschäftsmodell und sie kann ähnlich wie eine gewöhnliche Software einfach einsatzbereit erworben und direkt genutzt werden (Ransomware-as-a-Service).
- Eine Verschlüsselung kann zwar teilweise durch entsprechende Sicherheitssoftware erkannt und verhindert werden, jedoch folgen auf neue Erkennungsmechanismen auch stets neue Verschleierungstaktiken.

Phase der Erpressung

- Wichtige Daten sind verschlüsselt und Prozesse möglicherweise lahmgelegt. Für Entschlüsselung wird nun Geld erpresst typischerweise in einer Kryptowährung.
- Selbst bei Erfüllung der Zahlungsforderungen ist eine Entschlüsselung nicht immer gewährleistet.
- Es wird größtmöglicher Druck aufgebaut (Drohung mit Fristen und sich erhöhenden Auslösesummen sowie Drohung mit Veröffentlichung).
- Kooperationsunternehmen können ebenfalls von den Auswirkungen des Angriffs betroffen sein.

Erneute Erpressung

- An zuvor bezahltem Erpressungsgeld zeigt sich die Zahlungswilligkeit eines Unternehmens und es wird möglicherweise erneut zum interessanten Ziel.
- Weitere Erpressungen mit zuvor ausgeleiteten Daten sind möglich.
- Erneute Infiltration mittels einer „Backdoor“ ist möglich, falls das Unternehmensnetz nicht vollständig bereinigt wurde. Deshalb sollte das Unternehmensnetz in diesen Fällen immer neu aufgesetzt werden.

Checkliste: Was tun, wenn man Opfer wurde?

Sollte Ihre Organisation Opfer von Ransomware werden, empfiehlt das LSI anhand der folgenden Checkliste zu handeln.

Erkennung und Analyse

- ☐ Stellen Sie fest, welche Systeme betroffen sind und **isolieren** Sie diese umgehend.
  - Wenn mehrere Systeme oder Subnetze betroffen sind, und es nicht möglich ist einzelne Systeme zu isolieren, dann trennen Sie die Systeme oder das Netzwerk auf der Switch-Ebene.
  - Sollte es nicht sofort möglich sein, das Netzwerk an zentraler Stelle offline zu nehmen, trennen Sie die betroffenen Geräte durch Ziehen des Netzwerkkabels vom Netzwerk und schalten Sie den Flugzeugmodus an, um die Infektion einzudämmen.
  - Für den Fall, dass Sie Geräte aus irgendeinem Grund nicht vom Netzwerk trennen können, trennen Sie das Gerät vom Strom: nicht runterfahren, sondern von der Stromquelle trennen (z.B. Stromkabel ziehen, Akku/Batterien entfernen), um eine weitere Ausbreitung der Ransomware-Infektion zu vermeiden. (Hinweis: Ransomware-Infektionsartefakte und potenzielle Beweise im Arbeitsspeicher gehen in diesem Fall zwar verloren, aber eine Weiterverbreitung wird so verhindert).
  - Keinesfalls darf eine Anmeldung mit privilegierten Nutzerkonten (Administratorkonten) auf einem potenziell infizierten System erfolgen, während das System sich noch im Netzwerk befindet oder mit dem Internet verbunden ist!

- ☐ Kommunizieren Sie auf zweifelsfrei sicheren Kanälen, um die Angreifer nicht verfrüht darüber zu informieren, dass der Angriff entdeckt wurde.

- ☐ Binden Sie relevante interne Stellen in Form eines **Krisenmanagement-Teams** ein (Leitungsebene, ISB, IT-Leitung, Datenschutzbeauftragte, Juristen, Personal-/Betriebsrat, Presse- und Öffentlichkeitsarbeit).

- ☐ Das LSI empfiehlt generell die **Anzeige** eines Cyberangriffs bei der Polizei.

- ☐ Analyse betroffener Systeme zur Wiederherstellung: Planen und **priorisieren Sie** die Wiederherstellung basierend auf einer (bereits vorhandenen) vordefinierten Liste kritischer (wichtiger) Systeme. Identifizieren Sie die betroffenen kritischen Systeme zusammen mit den benötigten Daten, die wiederhergestellt werden müssen. Legen Sie den Wiederherstellungsplan der Organisationsleitung vor.

- ☐ Im Fall eines akuten Informationssicherheitsvorfalls, bei dem Erkennung, Beseitigung und Wiederanlaufplanung die Möglichkeiten und

Fordern Sie als Behörde, Kommune oder öffentliches Unternehmen im Bereich kritischer Infrastrukturen, wie Krankenhäuser oder Wasserversorger, Unterstützung des Bayern-CERT im LSI an (cert@bayern.de, 0911 21549 999)

Wichtige Informationen vorhalten:

- **Kontaktdaten**
- **Involvierte Parteien (betrifft sowohl betroffene als auch unterstützende)**
- **Zeitpunkt der Entdeckung**
- **Betroffene Systeme (Server/Client, Betriebssystem und Anwendung(en) inkl. deren Patchstände - soweit bereits bekannt)**
- **Bereits getroffene Maßnahmen**

Wir empfehlen bereits bei Verdacht auf einen Ransomware-Vorfall frühzeitig Unterstützung hinzuzuziehen.

Fähigkeiten der eigenen Organisation (evtl. auch kurzzeitig) überschreiten, muss geklärt sein, wie beispielsweise von externen IT-Sicherheitsdienstleistern **Hilfe angefordert** werden kann (z.B. Liste der „APT-Response-Dienstleister" des BSI). Es muss sichergestellt werden, dass der Dienstleister zur Einhaltung des Sicherheitsniveaus geeignete organisatorische und vertragliche Maßnahmen trifft.

- Lassen Sie die Organisationsleitung festlegen, wer die Presse- und Öffentlichkeitsarbeit übernimmt, um sicherzustellen, dass **nur zielführende Informationen** nach außen geteilt werden. Festgelegt werden muss auch, wer intern zu dem Sicherheitsvorfall informiert.

Hinweis: Das LSI rät generell von Lösegeldzahlungen ab. Die Zahlung von Lösegeld stellt nicht sicher, dass die Daten hinterher tatsächlich entschlüsselt werden können, dass die Systeme trotz einer Zahlung nicht erneut kompromittiert werden oder dass die erbeuteten Daten nicht dennoch veröffentlicht werden.

Schadensbegrenzung, Informationsbeschaffung und Beweissicherung

- Zur Gefahreneindämmung müssen alle möglichen **Kommunikationsverbindungen** zum Internet und zwischen Netzsegmenten **getrennt werden** (auch Übergänge zu VPNs, Fernzugriffsservern, Cloud-SSO-Ressourcen und cloudbasierten oder öffentlich zugänglichen Ressourcen).
- Ein Systemabbild (Festplattenimages inkl. Arbeitsspeicher) von betroffenen Geräten (Arbeitsplatzrechner, Server etc.) ist zu erstellen.
    - Daten aus volatilem Speicher sind aufzubewahren, um Verlust oder Manipulation zu verhindern (u.a. Systemspeicher, Windows-Sicherheitsprotokolle).
- Recherchieren Sie unbedingt nach möglichen Entschlüsselungswerkzeugen („Decryptor"), da Sicherheitsforscher Verschlüsselungsalgorithmen für einige Ransomware-Varianten bereits geknackt haben.
- Recherchieren Sie bei vertrauenswürdigen Quellen nach Informationen und besonderen Verhaltensweisen der Ransomware-Variante und befolgen Sie die zusätzlichen empfohlenen Schritte, um betroffene Systeme oder Netzwerke zu identifizieren und die Infektion mit der Ransomware einzudämmen.
- Der Infektionsweg ist zu analysieren und Systeme und Konten, durch welche die Ransomware eingeschleust wurde (z.B. über eine Phishing-Mail) sind zu identifizieren.

Sollten Sie eine Strafanzeige gegen die Angreifer in Erwägung ziehen, entstehen besondere Anforderungen an eine angemessene Beweismittelsicherung.

Hierzu unterstützt sie die **Zentrale Ansprechstelle Cybercrime (ZAC)** der bayerischen Polizei.

- ➔ Telefon: 089/1212-3300 (Bürozeiten: Mo-Do 08:00 – 16:00 Uhr und Fr 08:00 – 14:00 Uhr)
- ➔ Telefon außerhalb der Bürozeiten: Polizeinotruf 110
- ➔ Webauftritt: https://www.polizei.bayern.de/kriminalitaet/internetkriminalitaet/002464/index.html

Informieren Sie Ihren zuständigen Datenschutzbeauftragten über den Vorfall, falls der Verdacht besteht, dass personenbezogene Daten entwendet wurden.

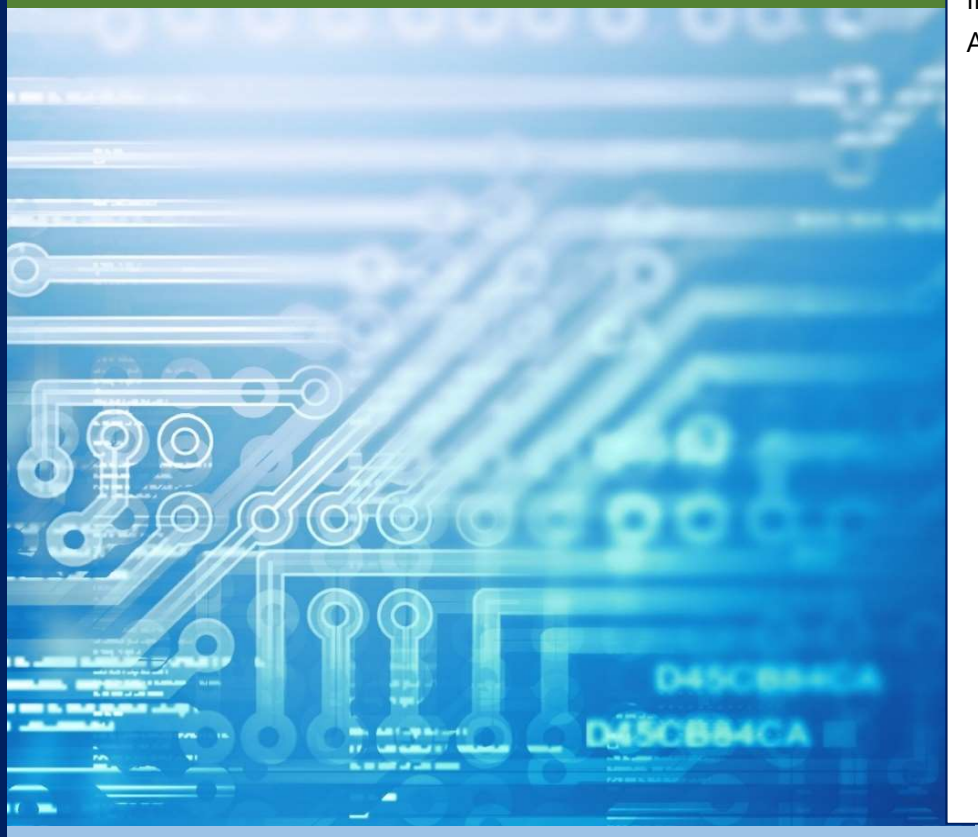
- Als weitere Sofort-Maßnahme sollten in diesem Fall unbedingt die identifizierten Konten unverzüglich deaktiviert werden.

- Analysieren Sie Protokolldateien von Erkennungs- oder Präventionssystemen (Antivirus, Intrusion Detection/Prevention Systeme, Firewalls, Web-Proxy, usw.). Dies kann Hinweise auf zusätzliche Systeme oder Malware geben, die an früheren Phasen des Angriffs beteiligt waren und/oder ebenfalls infiziert sind.

- Suchen Sie nach Hinweisen auf Vorläufer-Malware („Dropper-Malware"). Ein Ransomware-Angriff kann ein Hinweis auf eine frühere, unbemerkte Netzwerkkompromittierung sein. Viele Ransomware-Infektionen sind das Ergebnis bestehender Malware-Infektionen z.B. durch Qakbot, TrickBot, Dridex oder Emotet.

- Sammeln Sie alle relevanten Protokolle, welche IOCs beinhalten könnten: Active-Directory-, LDAP-Logs, Logs des HTTP-Proxy, Logs des E-Mail-Servers, Firewall-Logs, verdächtige Registry-Einträge, System-Logs oder andere relevante Dateien (z.B. um HTTP-Datenverkehr zu Command & Control Servern entdecken und nachvollziehen zu können).

Info: Bei IOCs handelt es sich um Artefakte, die Schadsoftware auf dem infizierten System hinterlassen. Hierzu gehören beispielweise ungewöhnlicher Datenverkehr im Netzwerk bzw. ins Internet, Anomalien beim Login, ungewöhnliche DNS-Anfragen oder verdächtige Änderungen in der Registry oder von Systemdateien. Sie finden sich oft in Logs und sind für die Forensik wichtig zur weiteren Analyse.



Übersicht: Die folgenden Informationen können für eine Analyse hilfreich sein:

- Ausführbare Dateien
- RAM-Abbilder
- Images von infizierten Systemen
- Malware-Dateien
- Verschlüsselte Dateien
- Log-Dateien (Windows Event Logs, Firewall Logs etc.)
- Auf dem System ausgeführte PowerShell-Skripte
- Im Active Directory angelegte Benutzeraccounts
- Von Angreifern genutzte Email-Adressen
- Kopie der Lösegeldforderung
- Bitcoin-Wallets der Angreifer

- Setzen Sie anhand des Wiederherstellungsplans die betroffenen Systeme neu auf, **beginnend mit kritischen Diensten**. Verwenden Sie auf jeden Fall neue Administrator-Passwörter.
- Verwenden Sie nur nachweislich **nicht kompromittierte Backups** oder sauber vorkonfigurierte Standardimages. Installieren Sie alle notwendigen Patches.
- Sobald die Umgebung vollständig bereinigt und neu aufgebaut wird, setzen Sie alle **Kennwörter** auf allen betroffenen Systemen einschließlich der Benutzeraccounts zurück.
- Die neu erstellten Systeme nach **Wiederherstellungsplan** mit dem Netzwerk verbinden und, falls notwendig, Daten aus Offline-Backups wiederherstellen.
- **Dokumentieren** Sie die Erkenntnisse, die Sie aus dem Vorfall gewonnen haben. Treffen Sie entsprechende Gegen- und Präventionsmaßnahmen. Falls nötig, aktualisieren Sie bestehende Unternehmensrichtlinien und Notfallpläne.
- Ziehen Sie in Betracht, die gemachten **Erfahrungen** mit anderen Organisationen zu **teilen**, um weiteren Ransomware-Angriffen vorzubeugen.

Hinweis: Stellen Sie sicher, dass während der Wiederherstellung keine neuen Infektionen erfolgen können (beispielsweise durch den versehentlichen Anschluss noch nicht bereinigter Systeme an das wiederhergestellte Netzwerk).

Backups

Backups sind für die Begrenzung eines Schadens durch einen Ransomware-Angriff essentiell. Sie sind der **einzig wirksame Schutz** vor vollständigem Datenverlust, da Daten bei Verschlüsselung schnell wiederhergestellt werden können. Deshalb sollten stets von allen wichtigen und wertvollen Daten Backups erstellt werden.

- Backups regelmäßig anfertigen und stichprobenartig auf ihre Funktion hin überprüfen.
- Nutzung einer Kombination aus Offline- und Online-Speichermethoden, um Datenverlust zu vermeiden.
- Daten auf einem oder mehreren physischen Geräten (z.B. Festplatten) oder verschlüsselt in Cloud-Speicherdiensten speichern und nach Möglichkeit unabhängig vom IT-Netz lagern. Bei einem Ransomware-Angriff können nicht nur lokale Daten verschlüsselt werden, sondern auch Daten, auf die von einem infizierten System aus zugegriffen werden kann. Bei Nutzung von Cloud-Diensten sollte ein „On Premise Backup" wichtiger Daten oder ein „Cloud to Cloud Backup" bei einem anderen Cloud-Anbieter in Erwägung gezogen werden.
- Die Speicherung auf einem externen Datenträger, der nach der Datensicherung vom Netzwerk getrennt wird, bietet die höchste Sicherheit vor Datenverlust.
- Zu einer guten Vorbereitung zählt ebenso die Erstellung und regelmäßige Pflege von Images kritischer Systeme, welche bei einem potentiellen Ransomware-Angriff neu aufgebaut werden müssen. Das Image sollte ein vorkonfiguriertes Betriebssystem (OS) enthalten, sowie zugehörige Softwareanwendungen, damit diese bei einem Neuaufbau der Systeme schnell wiederhergestellt werden können. Zusätzlich sollte ein Image des reinen Betriebssystems und separat die Installationspakete der genutzten Anwendungen aufbewahrt werden. Auf diese Weise kann auf einen möglichen Verlust der Vertrauenswürdigkeit einer einzelnen Anwendung umgehend reagiert und ein System ohne die verdächtige Anwendung neu aufgebaut werden.
- Nach einem erfolgten Ransomware-Angriff dürfen als möglicherweise noch infiziert zu betrachtende Geräte keinesfalls für eine Wiederherstellung der Betriebsfähigkeit genutzt werden. Stattdessen sollte auf bereits im Vorfeld beschaffte Ersatzhardware zurückgegriffen werden, um die Systeme schnell wieder neu aufzubauen. Ist die Hardware älter oder neuer als das primäre System, ist darauf zu achten, dass es nicht zu Kompatibilitäts- oder Installationsproblemen kommt.

Info: Backups sollten immer nach der 3-2-1-Backup-Regel erstellt werden. Gemeint ist damit das Erstellen von drei Datenkopien auf mindestens zwei unterschiedlichen Medien, wovon mindestens ein Backup sicher vom Netz getrennt gelagert werden sollte.

Weiterführende Informationen: LSI-Info Datensicherung (Backup und Recovery)

Authentifizierung

- Achten Sie auf eine ausreichende Komplexität bei der Wahl von Passwörtern in Ihrer Organisation (Passwortlänge und verschiedene Zeichenbereiche).
- Sensibilisieren Sie Ihre Mitarbeiter im Umgang mit Passwörtern.
- Zwei-Faktor-Authentifizierung entspricht mittlerweile dem Stand der Technik und ist gerade in kritischen Bereichen unbedingt zu nutzen. Sie ist Minimalvoraussetzung bei Fernzugriffen ins Unternehmensnetz und sollte auch bei Systemen und Accounts mit erweiterten Rechten genutzt werden.

Schlüsselpositionen

- Stellen Sie sicher, dass Mitarbeiter in Schlüsselpositionen über ausreichend Erfahrung in ihrem jeweiligen Aufgabengebiet verfügen.
- Mitarbeiter in Schlüsselpositionen sollten bei möglichen Vorfällen unbedingt verfügbar sein. Für Urlaub und andere Ausfallzeiten empfiehlt es sich qualifizierte Stellvertreter zu benennen.
- Auch die Stellvertreter der Schlüsselpositionen sollten über ausreichend Erfahrung verfügen.

Kooperationen aufbauen

- Errichten Sie bezüglich IT- und Informationssicherheitsthemen Kommunikationswege zu anderen Organisationen, Behörden oder Informationsportalen, welche Ihrer Branche angehören oder sich mit dieser Branche beschäftigen.

Weiterführende Informationen: LSI-Info Umgang mit Passwörtern

Reaktions- und Kommunikationsplan

Ein Reaktionsplan umfasst die **Vorgehensweise** bei einem Ransomware-Vorfall und beinhaltet einen Kommunikationsplan, der beschreibt welche Personen/Stellen wie zu informieren sind.

- Einen Reaktionsplan für den Eintritt eines IT-Sicherheitsvorfalls erstellen und „offline“ verfügbar machen.
- Dieser ist regelmäßig zu pflegen und sollte, ähnlich dem Verhalten bei einem Feueralarm, geübt und geprobt werden.
- Auch eine Pressemeldung für den Fall der Fälle kann vorbereitet werden.

Sensibilisierung

Die regelmäßige **Schulung von Mitarbeitern** ist essenziell, um das Risiko eines erfolgreichen Ransomware-Angriffs und den potentiell daraus entstehenden Schaden zu minimieren. Als besonders gefährdet gelten Abteilungen, in denen häufig E-Mail-Anhänge von unbekannten Absendern geöffnet werden müssen (z.B. Personalabteilungen). Allerdings ist auch beim Öffnen von E-Mails vermeintlich bekannter Absender stets auf Unregelmäßigkeiten zu achten. So könnte sich beispielsweise ein Angreifer Zugriff auf das Postfach des Absenders verschafft und vorhandene Mailinhalte in die Angriffsmail eingebaut haben. Mitarbeiter, welche in der Lage sind bösartige E-Mails/Links/etc. vor dem Öffnen zu erkennen, bieten einen signifikanten Sicherheitsgewinn für die IT einer Organisation.

- Schulungen sollen nicht nur Informationen zur Erkennung von potentiellen Gefährdungen beinhalten, sondern auch auf das korrekte Verhalten des einzelnen Mitarbeiters beim Verdacht auf einen Vorfall (Wer ist wie worüber zu informieren?) eingehen.
- Um Mitarbeiter zu sensibilisieren und das Bewusstsein für dieses Thema zu erhöhen, können organisationsweite Phishing-Tests durchgeführt werden.

Phishing

- Durch die Implementierung von Filtern am E-Mail-Gateway mit bekannten bösartigen Indikatoren (z.B. bestimmte Betreffzeilen, IP-Adressen, ausführbare Dateien als Anhang, etc.) können bereits im Vorfeld verdächtige E-Mails geblockt oder markiert werden. Die Filterung oder Markierung von verdächtigen E-Mails erhöhen somit die IT-Sicherheit einer Organisation.
- Soweit möglich, soll die Ausführung von Makros und von OLE-Objekten in Microsoft Office auf allen IT-Systemen unterbunden werden. Als Ausnahme sollte nur die Ausführung signierter und gegebenenfalls durch die IT-Abteilung geprüfter Makros freigegeben werden.

Phishing	Spear-Phishing
Es werden wahllos E-Mails an einen großen Empfängerkreis versendet, in der Hoffnung, dass einige Empfänger auf enthaltende Links klicken.	Die E-Mail ist speziell auf einen Empfänger zugeschnitten und wirkt oft täuschend echt, da sie nicht selten persönliche Informationen enthält.

Weiterführende Informationen: LSI-Info IT-Security-Awareness

Antiviren- und Anti-Malware-Software

Die beste technische Prävention gegen Ransomware-Angriffe besteht darin, der Malware keinen Zugang zum Computer zu bieten. Hierfür ist eine effektive Antivirus- und Anti-Malware-Software von höchster Qualität (z.B. Advanced Endpoint Detection and Response) mit einem starken Ransomware-Schutz zu installieren. Da ständig neue Ransomware-Varianten entwickelt werden, ist das Antivirus-Programm jederzeit auf dem **neuesten Stand** zu halten. Dies sollte automatisch erfolgen. Eine regelmäßige Kontrolle, ob die automatisierten Updates ordnungsgemäß installiert werden, ist anzuraten.

Hinweis: Eine Ransomware-Infektion kann auch ein Hinweis auf eine frühere, unbemerkte Netzwerk-Kompromittierung sein. So sind viele Ransomware-Infektionen das Ergebnis bestehender Malware-Infektionen, wie z.B. Qakbot, Emotet oder TrickBot. In manchen Fällen ist die Bereitstellung von Ransomware nur der letzte Schritt einer Netzwerk-Kompromittierung und wird zur Verschleierung vorheriger Aktivitäten genutzt.

- Grundsätzlich ist sicherzustellen, dass nur von der IT autorisierte Software ausgeführt werden kann. Jegliche nicht autorisierte Software ist vor der Ausführung zu blockieren (z.B. durch AppLocker).
- Die Implementierung von Intrusion Detection Systemen ist sinnvoll, um Command-and-Control-Aktivitäten und andere potenziell bösartige Netzwerkaktivitäten zu erkennen, welche bereits vor dem Ausrollen der Ransomware stattfinden können.

Weiterführende Informationen: LSI-Info IDS/IPS

Benutzerrechte

Ein weiterer Faktor zur Verhinderung einer Ransomware-Ausbreitung im Netzwerk kann die **restriktive Vergabe von Benutzerrechten** sein. Sind die Zugriffsmöglichkeiten von Mitarbeitern bereits auf Verzeichnisebene reduziert, kann eventuell die abteilungsübergreifende Verschlüsselung von Daten in einer Organisation verhindert werden.

- Bei der Vergabe von Benutzerrechten ist stets das Minimalprinzip anzuwenden, keinesfalls sollten normale Nutzer Adminrechte haben.
- Benutzer sollten keine Anwendungen installieren können.
- Sofern möglich, sollten auch die Zugriffsrechte von Software auf die notwendigen Verzeichnisse eingeschränkt werden. (z.B. Einschränkung auf Programme, Programme (x86), System32)

Info: Das Minimalprinzip besagt, dass Mitarbeiter nur die Berechtigungen erhalten, die für Ihre Tätigkeit zwingend notwendig sind.

Dienstleister (Managed Service Provider und sonstige Diensteanbieter)

Dienstleister können von Angreifern gezielt als Zwischenschritt auf dem Weg in das Unternehmensnetz genutzt werden. Sie bieten einen Angriffspunkt mit Auswirkung auf die eigene Organisation. Es ist vertraglich zu regeln und zu kontrollieren, dass Dienstleister mindestens dieselben Sicherheitsstandards erfüllen wie die beauftragende Organisation.

- Die Umsetzung der Vereinbarungen muss regelmäßig vom Auftraggeber kontrolliert werden.
- Vor Vertragsvergabe ist auf ein angemessenes Risikomanagement bei den Vertragspartnern zu achten und die Einhaltung dessen während der Vertragslaufzeit regelmäßig zu prüfen.

Eine entsprechende Regelung, z.B. bzgl. Backups, könnte als Anforderung im Dienstleistervertrag in der folgenden Form festgehalten werden: „**Backups sind regelmäßig zu erstellen, zu überprüfen und getrennt vom IT-Netz zu lagern.**“

Angreifer können das Vertrauen zwischen Dienstleistern und der eigenen Organisation für weitere Angriffsarten ausnutzen. So werden z.B. Dienstleister gezielt angegriffen, um Zugang auf Kundensysteme zu erhalten und diese mit Ransomware zu infizieren. Es besteht die Möglichkeit, dass Angreifer die Identität von gefälschten oder kompromittierten E-Mail-Konten verwenden, um so an notwendige Informationen einer Organisation zu gelangen oder das Organisationsnetzwerk zu kompromittieren (z.B. mit E-Mail-Anhängen von vermeintlich vertrauensvollen Absendern).

Eingesetzte Betriebssysteme oder Software

Viele Updates beinhalten **Sicherheitspatches**, welche vor Ransomware-Angriffen und anderer Malware schützen.

- Systemaktualisierungen müssen - je nach Kritikalität - so zeitnah wie möglich durchgeführt werden.
- Bei besonders betriebskritischen Systemen empfiehlt es sich, das Verhalten des Systems nach dem Patchen vorab auf einem Testsystem auf Funktionsfähigkeit zu prüfen.
- Veraltete Betriebssysteme und Software, welche nicht mehr mit regelmäßigen Updates versorgt werden, sind nach Möglichkeit auszutauschen oder im Netzwerk zu isolieren, da sie besonders anfällig für Angriffe sind. Aufmerksamkeit sollte ebenfalls auf die Aktualisierung von Webbrowsern und Plugins gelegt werden.
- Routinen zur regelmäßigen Überprüfung der Aktualität der Softwarestände sollten eingerichtet werden.

Für die sichere Konfiguration von eingesetzten Betriebssystemen bietet z.B. die Allianz für Cyber-Sicherheit auf ihrer Webseite Sicherheitsempfehlungen zu Windows, Apple OS X und Linux an.

Weiterführende Informationen: LSI-Info Patchmanagement

Schwachstellenscans und weitere Konfigurationen

Die **richtige Konfiguration** von Geräten und deren Sicherheitsfunktionen ist essentiell, um wirksamen Schutz vor Ransomware-Angriffen zu erhalten. Besonders gefährdet sind dabei Geräte, welche direkt aus dem Internet erreicht werden können.

- Um Schwachstellen identifizieren und beheben zu können, sind regelmäßig Schwachstellenscans durchzuführen mit dem Ziel, die Angriffsfläche nachhaltig zu verringern. Um einer möglichen Betriebsblindheit vorzubeugen, empfiehlt es sich, interne Scans durch externe zu ergänzen.
- Ungewöhnliches Systemverhalten sollte umgehend genauer analysiert werden.
- Es ist zu empfehlen, sämtliche Ports und Protokolle zu deaktivieren, welche nicht für die Funktion der Systeme notwendig sind und Log-Funktionen in angemessener Tiefe („Log-Level" konfigurieren) für verwendete Dienste zu nutzen.

Warn- und Informationsdienst (WID) des LSI:

Der WID des LSI informiert Sie

- **branchenorientiert**
- **anlassbezogen**
- **aufbereitet mit Empfehlungen**

über aktuelle IT-Schwachstellen und Gefährdungen.

Für die Staatsverwaltung, Kommunen und die öffentlichen Betreiber kritischer Infrastrukturen.

Anmeldung unter beratung-kritis@lsi.bayern.de

Als besonders kritisch ist das Server Message Block (SMB)-Protokoll hervorzuheben. SMB wird von Angreifern genutzt, um Malware über Organisationseinheiten hinweg zu verbreiten. Auf dieser spezifischen Bedrohung basierend, sollten Organisationen die Nutzung des SMB-Protokolls auf den internen Gebrauch beschränken und SMBv1 und SMBv2 im Organisationsnetzwerk deaktivieren. Zusätzlich sollte auf bestehende Abhängigkeiten zu Systemen oder Applikationen geachtet werden. Die Nutzung von veralteten Versionen von SMB sollte blockiert bzw. falls möglich, direkt auf den IT-Systemen, deaktiviert werden, um das Risiko der Verbreitung einer potentiellen Schadcodeinfektion zu reduzieren.

Angreifer erlangen oft über schlecht abgesicherte Remote-Dienste Zugang zum System und können so Ransomware verbreiten. Das Netzwerk ist daher auf Systeme zu prüfen, welche einen ungewollten direkten Remote-Zugang (RDP, VNC, etc.) aus dem Internet auf interne Systeme erlauben. Diese Konfigurationsfehler können z.B. mittels eines externen Schwachstellenscans entdeckt und im Anschluss behoben werden. Generell sind starke 2-Faktorauthentifizierungen bei Fernzugängen essentiell.

SMB nutzt die folgenden Ports:

- ➔ 137/TCP
- ➔ 137/UDP
- ➔ 138/UDP
- ➔ 139/UDP
- ➔ 445/TCP

Eingehende Verbindungen auf diese Ports aus dem Internet müssen blockiert werden.

Weitere Präventionsmaßnahmen

- Stellen Sie sicher, dass allen Mitarbeitern im Fall eines IT-Sicherheitsvorfalls ein Ansprechpartner bekannt und dieser entsprechend verfügbar ist.
- Generell empfiehlt es sich, die Dokumentation der eigenen IT-Infrastruktur stets auf dem neuesten Stand zu halten und in regelmäßigen Abständen zu kontrollieren, ob dies auch der Fall ist.
- Wichtige Dokumente oder Informationen, wie etwa Telefonlisten, Dokumentationen, etc. müssen auch bei einem IT-Sicherheitsvorfall zugänglich sein und sollten daher zusätzlich in ausgedruckter Form zur Verfügung stehen.
- Regelmäßige Schwachstellenscans von innen und von außen helfen, zeitnah Risiken zu erkennen, damit diese schnell beseitigt werden können. Hier kann es durchaus Sinn ergeben, einen Dienstleister damit zu beauftragen.
- Es sollten starke Passwörter verwendet werden und diese sollten auch nur für einen Account/Dienst genutzt werden. 2-Faktorauthentifizierung ist, wenn technisch möglich, zu bevorzugen. Ungenutzte Accounts sollten entfernt werden.
- Um für den Fall der Fälle gut vorbereitet zu sein, sollte bereits im Vorfeld die Verfügbarkeit benötigter Dienstleister vertraglich geregelt werden.
- Es empfiehlt sich auch, regelmäßig den Reaktionsplan auf Informationssicherheitsvorfälle zu überprüfen und mit dem vorab festgelegten Krisenmanagement-Team praxisnah zu üben.
- Außerdem sollte Ihre Organisation einen Netzplan (vgl. Abbildung 1) entwickeln und regelmäßig aktualisieren, der alle Systeme und Verbindungen aufzeigt. Im Ernstfall bietet dieser schnell und übersichtlich hilfreiche Informationen. Aus diesem Plan sollten die allgemeine Netzwerktopologie sowie IP-Adressschemata hervorgehen.

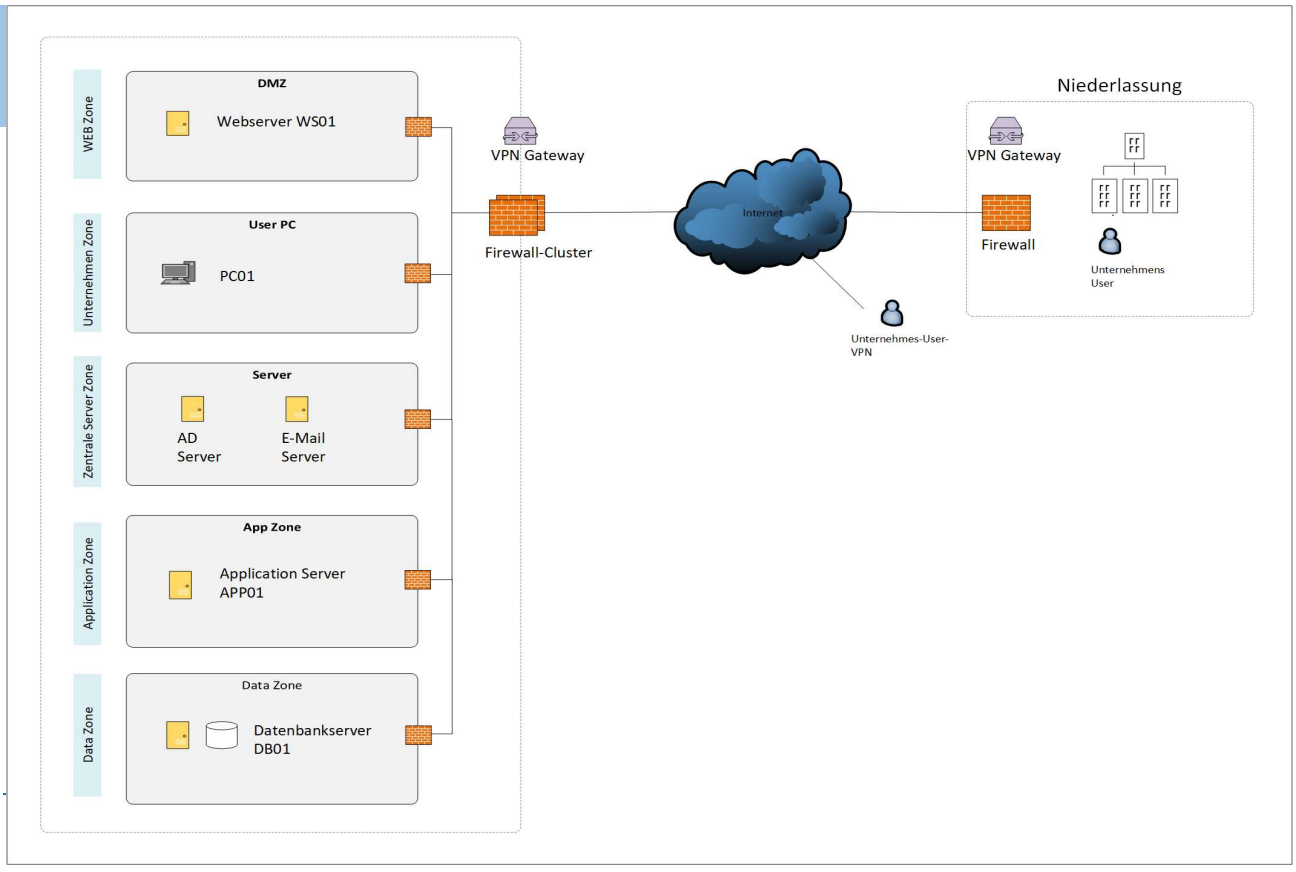


Abbildung 1: Netzwerk beispielhaft aufgeteilt in Sicherheitszonen

Es empfiehlt sich, das Organisationsnetzwerk nach Organisationseinheiten zu segmentieren (hauptsächlich durch Firewalls). Beispielsweise sollte das Verwaltungsnetz stets vom Betriebsnetz getrennt sein. Die folgenden beiden Abbildungen zeigen ein flaches Netzwerk und ein segmentiertes Netzwerk. Letzteres sollte stets die Wahl Ihrer Organisation sein, da dadurch „lateral movement“ eingedämmt oder sogar ganz verhindert werden kann.

Abbildung 2: Flaches unsegmentiertes Netzwerk (veraltet, unsicher)

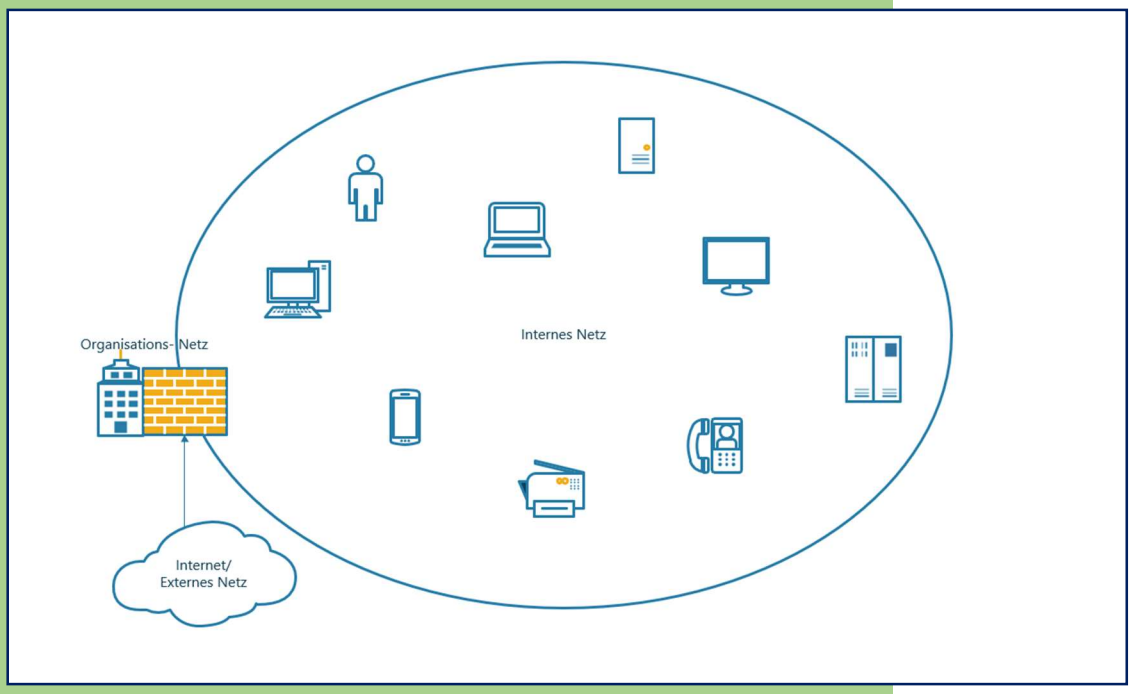
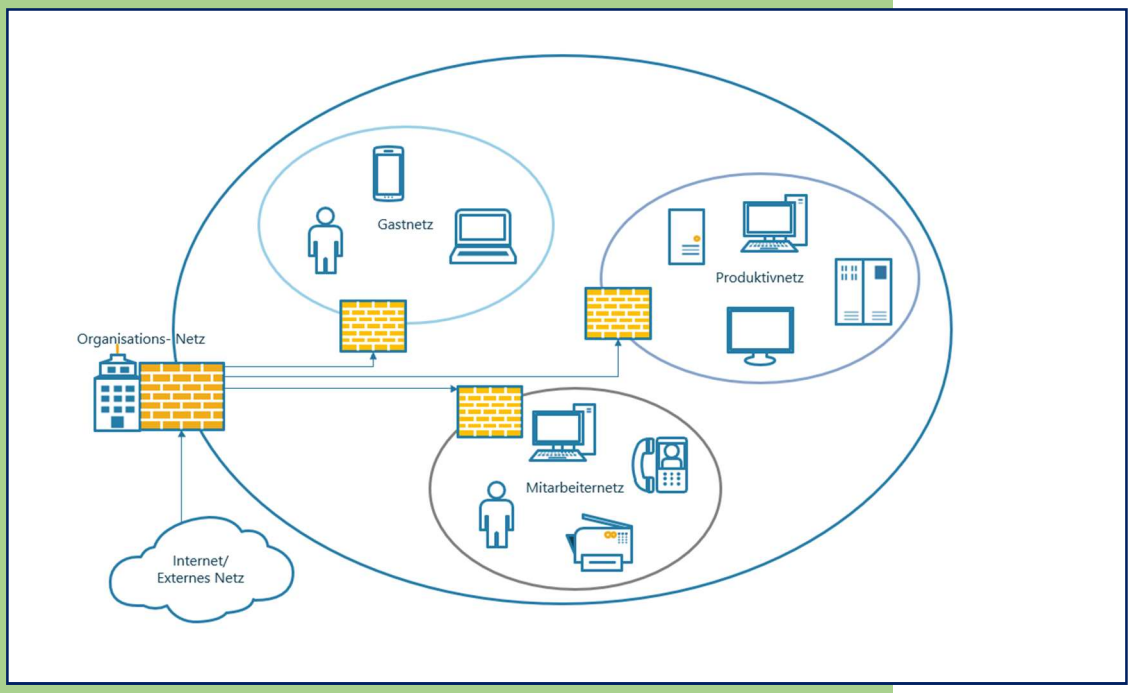


Abbildung 3: Segmentiertes Netzwerk



- Inventarisieren Sie Ihre Soft- und Hardware. Dies hilft dabei den Überblick über die verwendeten Geräte und Dienste zu behalten.

- Schränken Sie die Nutzung von PowerShell auf ausgewählte Benutzer mittels Gruppen-Richtlinien ein. Lediglich Administratoren sollten PowerShell nutzen können. Außerdem sollte hierbei auf ausreichendes Logging geachtet werden.

Sämtliche PowerShell Aktivitäten werden im Windows Event Log „PowerShell" und dem „PowerShell Operational" Log aufgezeichnet. Diese Logs sollten angemessen lange aufbewahrt werden.

- Domänencontroller sollten regelmäßig gepatcht werden. Aufgrund ihrer Rolle im Netzwerk sind sie besonders gefährdet, da sie als Ausgangspunkt für einen Ransomware-Angriff genutzt werden können. Es sollte keine zusätzliche Software auf diesen Systemen installiert sein. Des Weiteren sollten aktuelle Versionen von Windows Server genutzt werden, da hier bessere Sicherheitsfunktionen für das Active Directory vorhanden sind.

Für weitere Informationen steht Ihnen das Beratungsteam des LSI für Kritische Infrastrukturen gerne zur Verfügung.

- **E-Mail: beratung-kritis@lsi.bayern.de**
- **Telefon: 0911 21549-525**

Die Beratung für Kommunen erreichen Sie über:

- **E-Mail: beratung-kommunen@lsi.bayern.de**
- **Telefon: 0911 21549-523**