Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Maßnahmenkatalog Ransomware

Arbeitspapier

Änderungshistorie

Tabelle 1 Änderungshistorie

Version	*Datum*	*Beschreibung*
1.0	23.02.2022	Initialveröffentlichung

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Internet: https://www.bsi.bund.de
Service-Center (Telefon): 0800 2741000
Service-Center (E-Mail): service-center@bsi.bund.de
Einen Vorfall melden: https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/IT-Sicherheitsvorfall/Unternehmen/Online-Meldung/online-meldung_node.html
Für die Zielgruppen und Partner des BSI gelten darüber hinaus die üblichen Meldewege.

Vorwort

Dieses Arbeitsdokument dient zur Vorbereitung auf einen Ransomware-Angriff und stellt die notwendigen präventiven Grundlagen vor. Es wurde auf Basis der Erfahrungen, die bei der Ransomware-Fallbearbeitung gewonnen wurden, erstellt. Es richtet sich an Unternehmen und Behörden, die sich mit dem Thema noch nicht oder nur ansatzweise auseinandergesetzt haben und eine Übersicht über mögliche Schutzmaßnahmen vor Ransomware suchen. Das Dokument ist in zwei Teile gegliedert: Der erste Teil beschäftigt sich mit den wichtigsten Fragen für die Geschäftsführung bzw. Amtsleitung in Kapitel 1. Anschließend werden die maßgeblichen Maßnahmen zur Vorbeugung eines Ransomware-Vorfalls beschrieben. Abschließend wird in Kapitel 7 eine grobe Abschätzung zu Nutzen und Aufwand gegeben. Als kurzfristige Maßnahmen zum Schutz vor Ransomware wird insbesondere auf die Kapitel „Backups“ und „Bereiten Sie sich auf einen Vorfall vor“ verwiesen.

Dieses Dokument ersetzt nicht das systematische Herangehen an das Thema „Informationssicherheit.“ Ausführliche Informationen zum Schutz der Systeme hat das BSI im IT-Grundschutz veröffentlicht. Die meisten Ransomware-Angriff gehen neben der reinen Verschlüsselung von Daten auch mit Datenabfluss und Drohung der Veröffentlichung einhergehen. Nur eine ganzheitliche Herangehensweise bietet einen angemessenen Schutz vor „Fortschrittlichen Angriffen“ [1]. Punktuelle Maßnahmen wie in diesem Dokument dargestellt schützen hiervor nicht in vollem Umfang.

Gegen Schadprogramme und Ransomware im Speziellen gibt es nicht „die eine“ Maßnahme, welche hilft sich vor Produktionsausfall oder Datenverlust zu schützen. Vielmehr greifen viele Maßnahmen ineinander, welche zusammen umgesetzt werden müssen, damit die Aussicht besteht, einen Angriff an möglichst vielen Stellen auf dem Weg von der ersten Infektion eines Systems bis zur Verschlüsselung von IT-Systemen zu stoppen oder zumindest zeitnah zu entdecken („defense in depth“). Zwischen dem Eindringen in die IT-Systeme und einer Verschlüsselung liegen immer wieder Wochen, manchmal sogar Monate. Welche Maßnahmen konkret umgesetzt werden können und müssen, kann aber nicht pauschal vorgegeben werden, sondern erfordert immer eine Einzelfallbewertung.

Die Behörden- und Unternehmensleitung muss im Vorfeld gemeinsam mit dem Informationssicherheitsbeauftragten und den Fachleuten festlegen, welche Geschäftsprozesse für ihr Unternehmen bzw. ihre Behörde kritisch sind.
Entsprechende Verantwortliche können sich an den Fragen und Antworten aus Kapitel 1 orientieren, um ihrer Verantwortung und Haftungsrolle gerecht zu werden. Diese sollten regelmäßig gestellt und beantwortet werden. Kurzfristig besonders hilfreiche Maßnahmen (Quick-Wins) sind gekennzeichnet.

Das Dokument enthält Informationen für die Vorbereitung und Beantwortung der aufgeworfenen Fragen durch CISO, IT-Betrieb und / oder IT-Dienstleister.

Ransomware ist aktuell eine reale, ersthafte Bedrohung mit vielen weiteren Betroffenen bei den entsprechenden Kunden, Partnern und Lieferanten, die außerdem große Medienaufmerksamkeit nach sich ziehen kann. Die Wahrscheinlichkeit, dass auch Ihr Unternehmen / Ihre Behörde getroffen wird ist derzeit hoch und realistisch. Die Konsequenzen sind mitunter so schwerwiegend, dass Prävention wirtschaftlicher sein sollte, als den eintretenden Schaden in Kauf zu nehmen. Je nach Unternehmensgröße liegt dieser z.T. im Multi-Millionenbereich. Es sollte auch bedacht werden, dass Cyber-Versicherungen in ihren Versicherungsbedingungen konkrete IT-Sicherheitsmaßnahmen (z.B. ein geeignetes Backup-Konzept) vorgeben und im Schadensfall sehr genau auf Versäumnisse des Versicherungsnehmers prüfen. Im Rahmen Ihrer (Mit-) Verantwortung müssen Sie agieren. Sollten Sie sich bereits gut aufgestellt fühlen, nutzen Sie die Empfehlungen, Ihre Maßnahmen erneut zu überprüfen und ggf. zu verbessern.

Ransomware ist keine „Höhere Gewalt“.

Höhere Gewalt ist ein von außen kommendes, unvorhersehbares und unbeherrschbares, außergewöhnliches Ereignis, das auch durch äußerste Sorgfalt nicht verhütet bzw. abgewendet werden kann. - wirtschaftslexikon.gabler.de *[2]*

Die Beschreibung „Höhere Gewalt“ trifft in aller Regel nicht auf Ransomware zu. Etwas anderes mag in seltenen Einzelfällen bislang unbekannter, neu entwickelter Ransomware gelten.
Für den Regelfall gilt aber, dass es regelmäßig erfolgreiche Angriffe auf Unternehmen, Behörden und IT-Dienstleister aller Größen gibt, über welche oftmals medial durch Tagespresse berichtet wird. Mit entsprechenden Maßnahmen können diese durchaus verhindert bzw. die Eintrittswahrscheinlichkeit eines großen Vorfalls erheblich gesenkt werden. Die Auswirkungen können mit entsprechenden Präventivmaßnahmen besser beherrscht werden.

Inhalt

1 Prüf-Interview

Dieses Kapitel enthält für die Geschäftsführung bzw. die Amtsleitung eine Sammlung relevanter Musterfragen sowie für den IT-Betrieb entsprechende exemplarische Musterantworten.

Gibt es ein Backup-Konzept? Sind Backups im Normalfall nicht über das Netzwerk erreichbar? (Quick-Win)

Ein Backup-Konzept wurde erstellt und mit den relevanten Stellen (z.B. Fachverfahrensverantwortlichen) abgestimmt.

Es werden regelmäßig Backups der wichtigsten Daten und Systeme erstellt. Dabei handelt es sich um die folgenden IT-Systeme (alle kritischen Geschäftsprozesse sind abgedeckt): [...]

Backups sind nicht dauerhaft mit dem IT-Netz verbunden, sondern nur während der Zeit des Backup-Vorgangs. Es werden mehrfache Kopien der wichtigsten Daten auf unterschiedlichen Backup-Lösungen erstellt. Diese werden separat an unterschiedlichen Standorten gelagert. Die Daten können aus den Backups wiederhergestellt werden. Die Wiederherstellung von Daten und Systemen wird regelmäßig geübt.

Sind auf extern erreichbaren Systemen die aktuellsten Patches aufgespielt, und somit alle Schwachstellen behoben? Wenn nicht, welche alternativen Maßnahmen werden zum Schutz getroffen? (Quick-Win)

Veröffentlichte Updates und Patches in allen extern erreichbaren Systemen werden schnellstmöglich eingespielt.[1] Die Patchstände werden regelmäßig überprüft. Wo Patches derzeit nicht aufgespielt werden können, wurde dies mit den entsprechenden zusätzlichen Schutzmaßnahmen dokumentiert. Diese Ausnahmen werden regelmäßig geprüft. Ausnahmen welche aufgrund operativer Fachverfahren nötig sind, wurden den Fachverfahrensleitenden mitgeteilt sowie dem Vorstand zur Kenntnis gegeben

Welche Netzbereiche werden von uns genutzt? Werden diese zentral verwaltet?

Uns sind die folgenden Netzbereiche zugewiesen: [...]

Es ist Vorgabe und gelebte Praxis, dass Netzbereiche zentral beschafft und gemanaged werden. Sollten diese in Ausnahmefällen dezentral beschafft werden, wird der IT-Betrieb zeitnah eingebunden. Hierdurch haben wir eine Übersicht über besonders kritische Systeme und mögliche Angriffspunkte.

Welche Systeme sind von außen erreichbar? Ist dies zwingend erforderlich? (Quick-Win)

Von außen sind lediglich der Webserver sowie der Mailserver - zum Empfang und Versand von E-Mail - ohne zusätzliche Schutzmaßnahmen erreichbar. Außerdem sind noch die folgenden Systeme freigegeben: [...] Dabei sind jeweils nur die zwingend notwendigen Ports freigegeben. Dies ist unbedingt erforderlich und nicht umgehbar. Die Gründe dafür sind dokumentiert. Insbesondere sind häufig angegriffene Dienste wie RDP oder OWA deaktiviert oder nur über VPN erreichbar. Die Einschränkung auf zwingend notwendige Ports wird regelmäßig geprüft.

Wird grundsätzlich VPN für die Verbindung zu internen Systemen verwendet?

Externe Verbindungen auf interne Systeme sind nur von bekannten IPs oder über VPN erlaubt. VPNs werden über Multi-Faktor-Authentisierung geschützt und es erfolgt ein Monitoring der Zugriffe. Alle Ausnahmen wurden in der Frage zuvor dargestellt.

[1] Nach Kenntnis des BSI sind regelmäßig tausende Systeme in Deutschland für Kritische Schwachstellen verwundbar. Wenn für Systeme bereits Wochen oder Monate Patches bereitstehen, könnte man sich damit im Bereich der Fahrlässigkeit bewegen.

Wie werden administrative Zugänge geschützt? Wie ist der Stand für alle weiteren Zugänge?

An allen externen Zugriffspunkte wird Multi-Faktor-Authentifizierung verwendet, insbesondere für alle administrativen Zugänge.

Es haben nur eine kleine Anzahl von Administrierenden hoch privilegierte Konten im Active Directory. Für die Administration nutzen diese getrennte, besonders geschützte Clients, auf denen keine gewöhnlichen Bürotätigkeiten durchgeführt werden.

Verwenden die Administratoren getrennte Accounts für die Verwaltung von Clients und Servern?

Administratoren verwenden für E-Mail und Surfen im Netz, für die Administration der Clients und für die Administration der Server jeweils getrennte Accounts nur mit den notwendigen Berechtigungen und keine Domänen-Administrationsaccounts.

Wird die Ausführung von Programmen, Skripten und Makros eingeschränkt? (Quick-Win)

Scripting Umgebungen und Makros sind deaktiviert. Wo dies nicht möglich ist werden diese eingeschränkt und nur die Ausführung von signierten Makros ist erlaubt. Dies wird über Gruppenrichtlinien sichergestellt.

Trotz aller Maßnahmen ist es möglich, dass Schadprogramme die IT-Systeme erreichen. Daher wird zusätzlich verhindert, dass diese auf den Systemen ausgeführt werden können. Hierfür werden IT-Geräte zentral verwaltet und nur vom IT-Betrieb freigegebenen Programmen wird erlaubt, auf dem jeweiligen Gerät zu laufen, etwa mittels der Anwendungskontrolle „Application Whitelisting“. Wo dies noch nicht möglich ist wird alternativ als Basismaßnahme die Ausführung von Programmen auf nicht durch den Benutzer beschreibbare Verzeichnisse beschränkt (Application Directory Whitelisting).

Sind wir auf einen Vorfall vorbereitet? Sind alle kurzfristigen Eskalationsmechanismen festgelegt und bekannt? (Quick-Win)

Die Reaktion des IT-Betriebs auf einen Vorfall wurde für verschiedene Szenarien der Kompromittierung geplant. Eine Business-Impact-Analyse wurde in Abstimmung mit den Fachbereichen und der Behörden- / Unternehmensleitung erstellt und wird regelmäßig aktualisiert. Die Fachbereiche und die Leitung wurden auf nötige weitere Vorbereitungsmaßnahmen wie Kommunikationsstrategie und Listen zwingender Kontakte hingewiesen. Dies wurde dort auch umgesetzt.

Falls Webserver, Mailserver oder weitere Systeme wegen eines Vorfalls kurzfristig vom Netz getrennt werden müssen, sind dafür Handlungsoptionen (z.B. Ersatzsysteme) und Kommunikationspläne z.B. für Presse, Kunden und Partner vorbereitet.

Entsprechende Notfall-Dokumente wurden zusätzlich zu den üblichen Speicherorten noch ausgedruckt an zentraler Stelle, bekannt für alle Beteiligten, hinterlegt.

Die Pläne wie das „große Playbook“[2] und das technische Wiederherstellen werden regelmäßig geübt.

Welche Geschäftsprozesse sind kritisch? Welche Systeme sind dafür zwingend notwendig?

Von den Fachbereichen wurden die folgenden Geschäftsprozesse als kritisch festgelegt: [...]

Dafür sind aus Sicht des IT-Betriebs die folgenden Systeme zwingend erforderlich; [...]

Diese Liste wurde nochmals mit den Fachbereichen abgestimmt, um sicherzustellen, dass keine Systeme übersehen wurden.

[2] Vorgefertigter praktischer Ablaufplan, der möglichst detailliert das Vorgehen beim Auftreten bestimmter Vorfälle beschreibt. Darin werden die beteiligten Akteure, Kommunikationswege und das technische, praktische Vorgehen festgelegt.

2 Backups

Ein Backup ist die wichtigste Schutzmaßnahme, mit der im Falle eines Ransomware-Vorfalls die Verfügbarkeit der Daten und eine schnelle Wiederaufnahme des Betriebs gewährleistet werden kann. Jede Institution sollte über ein Datensicherungskonzept (siehe IT-Grundschutz Kompendium: CON.3. Datensicherungskonzept [3]) verfügen und dieses auch umsetzen.

Hierbei gibt es viele verschiedene Möglichkeiten für Backups, etwa in einer Cloud, mit NAS, etc.
Je nach Einsatzzweck und Unternehmensgröße kann es sinnvoll sein, auch nur Daten auf Servern und Netzlaufwerken zu sichern und Clients im Fall einer Infektion neu aufzusetzen. Sofern Unternehmensdaten nur auf den Netzlaufwerken gespeichert sind, gehen dabei auch keine (langfristig) relevanten Daten verloren.
Auch muss geprüft werden, ob es genügt, nur die Inhaltsdaten zu sichern oder ob auch die Konfiguration gesichert werden sollte.

> *Es ist inzwischen bei Schadprogramm-Infektionen üblich, dass Angreifende mit zuvor erlangten Administrationsrechten gezielt nach allen Backups suchen und diese, ebenso wie Produktivsysteme, verschlüsseln.*

Daher sollte zumindest je eine Kopie offline gesichert werden. Diese Kopien werden nach dem Backup von den anderen Systemen der Einrichtung getrennt und sind daher vor Remote-Angriffen geschützt. Offline-Backups können etwa mit getrennten Tapes, in einem getrennten Archiv mit nötigem physischem Zugriff oder auch in einem komplett vom eigenen Netz getrennten Cloud-Speicher erfolgen.
Diese Trennung sollte auch regelmäßig überprüft werden. So könnte etwa ein (Domänen-) Administrierenden testweise versuchen, auf diese getrennten Backup-Kopien zuzugreifen. Dies sollte nicht gelingen.

Zusätzlich zur Resilienz vor Ransomware, bieten Backups auch Schutz vor physischen Beeinträchtigungen, etwa durch einen Brand, Hochwasser oder kurzfristiger Evakuierung. Daher sollten Kopien der Backups auf verschiedene geographische Orte verteilt werden.

Zu einem Backup gehört auch immer die Planung und Vorbereitung des Wiederanlaufs und der Rücksicherung der Daten. Diese Planungen sollten auch einem regelmäßigen Praxistest unterzogen werden, um Komplikationen und Herausforderungen in der Rücksicherung bereits vor einem Ernstfall zu erkennen. Ein Schwarzstart, d.h. ein Wiederanlauf aller Server und Systeme, sollte ebenfalls geplant und geübt werden.

Vor der Wiederherstellung sollte überprüft werden, ob die Backups bereits mit Malware infiziert sein könnten. Grundsätzlich sollte beim Wiederherstellen mit Kopien der Backups oder einem Write-Blocker gearbeitet werden, insbesondere, wenn nicht ausgeschlossen werden kann, dass die Systeme nicht doch mit Malware infiziert sind. Angreifer bewegen sich nach der initialen Infektion teilweise mehrere Wochen im Netzwerk und könnten daher bereits ins Backup aufgenommen worden sein.

> *Bitte beachten Sie, dass damit nur die Auswirkungen eines erfolgreichen Ransomware-Angriffs gemildert werden können. Daneben kopieren Angreifende bei entsprechenden Ransomware-Angriffen auch verschiedene Daten und drohen mit der Veröffentlichung dieser. Naturgemäß können Backups hiervor nicht schützen. Stattdessen gilt: Nur die Daten, die auch gespeichert werden, können abfließen. Je weniger Daten vorliegen, desto weniger können Angreifende damit drohen. Das gilt beispielsweise für historische Daten, Verläufe, ältere Kundendatenbanken, etc.*

3 Prävention vor Malware (Server Einstellungen)

Systeme können üblicherweise über E-Mails mit Schadprogrammen oder verwundbaren extern erreichbaren Systeme infiziert werden. Hier gibt es eine Reihe von möglichen Maßnahmen, diese wurden etwa im Rahmen der BSI-Empfehlungen rund um den Schutz vor Emotet [4] auch zuvor schon aufgeführt.

3.1 Umgang mit E-Mails

Die Wahrscheinlichkeit, dass E-Mails mit Schadprogrammen die Nutzer erreichen, kann beispielsweise durch folgende Maßnahmen reduziert werden:

- Spam sollte gefiltert und/oder markiert werden.
- Anhänge auf erwartbare Dateitypen filtern (mit positiv oder negativ Abgleich). Entsprechende E-Mails entweder blockieren, in Quarantäne verschieben oder geeignet markieren (z.B. [VERDÄCHTIGER ANHANG]). Beispiele für potentiell gefährliche Anhänge sind (nicht abschließend): .exe, .scr, .chm, .bat, .com, .msi, .js, .jar, .cmd, .hta, .pif, .scf, (verschlüsselte) Archiv/Zip-Dateien, MS-Office-Dokumente mit Makros (MIME/HTML-Kodierung betrachten). Je nach Dokumentenart könnten diese auch in andere Dateitypen umgewandelt werden, um Skripte und Makros zu deaktivieren (etwa Office-Dokumente in PDF-Dokumente).
- bekannte Schadprogramme prüfen und ggf. blockieren, z.B. mit AV-Signaturen. Die beste Detektionsleistung wird erreicht, wenn E-Mail-Anhänge mit einer Sandbox-Analyse überprüft werden.
- Links ggf. umschreiben, damit Nutzer diese wirklich bewusst aufrufen müssten.
- Die Implementierung und Prüfung von SPF, DKIM, und DMARC-Server hilft, bereits die Annahme von nicht legitimen E-Mails zu reduzieren. Hierbei ist jedoch zu prüfen, ob signifikante Seiteneffekte auftreten, die eigentlich gewünschte E-Mail-Kommunikation unterbinden. Auch hier kann schrittweise vorgegangen werden, etwa indem anfangs die DMARC policy ‚None' gesetzt wird und die Ergebnisse ausgewertet werden.
- E-Mail-Server sollten von extern eingelieferte E-Mails mit Absenderadressen der eigenen Organisation (sei es im Envelope-Header, im From-Header oder im Anzeigenamen) ablehnen, in Quarantäne verschieben oder mindestens im Betreff deutlich markieren (Anti-Spoofing).
- Blacklisting von (potentiell) schadhaften Mailservern.

Diese Punkte können entweder selbst umgesetzt und aktuell gehalten werden oder durch entsprechende E-Mail-Security-Gateways abgedeckt werden. Die Architektur entsprechende Gateways ist vielfältig, einige gibt es als lokal installierte Hardware, andere als lokal installierte virtuelle Lösung und wieder andere als Cloud-Lösung.

Neben dem direkten Versand von beispielsweise Office-Dokumenten mit Makros werden regelmäßig mit entsprechenden Spam-Mails auch nur Links verteilt, von deren Endpunkten dann die Office-Dokumente heruntergeladen werden. Hier hilft in beiden Fällen die Deaktivierung von (unsignierten) Makros, vgl. 4.1.

3.2 Extern erreichbare Systeme

Neben Angriffen über E-Mails erlangen Angreifende häufig auch Zugriff über schlecht gesicherte exponierte Dienste oder verwundbare extern erreichbare Systeme[3]. Voraussetzung für zielgerichtete Maßnahmen in diesem Bereich ist, dass eine Übersicht über entsprechende erreichbare Systeme besteht. Hierfür sollten bestehende Systeme zentral abgefragt und neue Systeme gemeldet werden.

[3] Aus Sicht des BSI sind nicht extern erreichbare Systeme, welche nicht schnell und ausreichend aktualisiert werden, eine der häufigsten Angriffsvektoren für Ransomware-Angriffe.

Zur Absicherung dieser Systeme gibt es verschiedene Maßnahmen.

3.2.1 Aktives Schwachstellenmanagement

Um generell vor Infektionen durch die Ausnutzung bereits behobener Sicherheitslücken geschützt zu sein, sollten Updates für extern erreichbare Systeme unverzüglich nach der Bereitstellung durch den jeweiligen Softwarehersteller getestet und eingespielt werden. Wenn der Betrieb der IT-Systeme durch einen externen Dienstleister erfolgt, sind SLAs ggf. gestaffelt nach Kritikalität der Updates zu vereinbaren.

Wo Patches derzeit nicht aufgespielt werden können, müssen zusätzliche Schutzmaßnahmen implementiert und dies dokumentiert werden. Diese Ausnahmen sollten regelmäßig geprüft werden.

In diesem Zusammenhang ist auch ein IT Asset Management inklusive einer jederzeit verfügbaren Übersicht über die jeweiligen Versionen der Hard- und Software geboten. Damit kann sich eine Behörde oder ein Unternehmen leichter einen Überblick über die jeweiligen Systeme verschaffen und feststellen, an welchen Stellen Handlungsbedarf besteht. Dies kann auch helfen Updates geeignet zu priorisieren. Hier gibt es unterschiedliche Ausgestaltungen, anfangs etwa in Form einer Excel-Tabelle bis hin zu Systemen, welche automatisch Hardware im Netzwerk erkennen.

3.2.2 Freigabe nur notwendiger Dienste und Ports

Von außen sollten grundsätzlich lediglich der Webserver sowie der Mailserver - zum Empfang und Versand von E-Mail erreichbar sein. Dabei dürfen nur die zwingend notwendigen Ports für diese Server freigegeben werden. Dienste wie beispielsweise RDP oder OWA sollten deaktiviert oder nur über VPN erreichbar sein. Die Einschränkung auf zwingend notwendige Ports sollte regelmäßig geprüft und möglichst über Penetrationstests getestet werden.

3.2.3 Remote-Zugänge absichern

Angreifende versuchen häufig Ransomware über kompromittierte Remote-Zugänge auf Systemen zu installieren. Daher sollte der Zugriff von außen abgesichert werden. Diese Zugänge sollten immer durch Authentisierung z.B. mittels VPNs - zusammen mit einer Multi-Faktor-Authentisierung - geschützt werden. Zusätzlich können auch Quell-IP-Filter und ein Monitoring die Absicherung unterstützen.

Darüber hinaus erfolgen Verbindungsversuche auf ein Netzwerk häufig auch über das Erraten von Passwörtern Daher sollte insbesondere bei Remote-Zugängen, die nicht über VPN abgesichert sind, eine wirksame Account-Lockout-Policy bestehen, um die Wahrscheinlichkeit eines erfolgreichen Brute-Force-Angriffs zu minimieren.

Bei der Absicherung von außen helfen auch Penetrationstests (siehe unten), die von außen öffentlich erreichbare Systeme identifizieren und auf ihre Sicherheit prüfen können.

3.2.4 Sicherer Umgang mit Administrator Accounts

Mit privilegierten Accounts sollten ausschließlich Administrationstätigkeiten durchgeführt werden. Insbesondere die Domänen-Administrationskonten sollten auf eine möglichst kleine Anzahl von Administrierenden begrenzt werden. Für die Administration sollten möglichst abgesicherte Clients genutzt werden, die auf keinen Fall für die Bearbeitung von gewöhnlichen Bürotätigkeiten wie die Bearbeitung von E-Mails oder das Surfen im Internet genutzt werden sollten. Für diese Tätigkeiten sollten Administrierende einen normalen Client mit einem normalen Nutzerkonto verwenden.

Ein privilegiertes Konto sollte immer über eine Multi-Faktor-Authentisierung geschützt werden. Für die Administration von Clients und Servern sollten keine Domänen-Administrationskonten verwendet werden.

Die Anmeldung als Administrator kann für bestimmte Systeme, z.B. Domänencontroller, auf sichere Arbeitsstationen / Privileged Access Workstations (PAWs) beschränkt werden.

3.3 Veraltete Systeme isolieren

Es kann verschiedene zwingende Gründe geben, warum Systeme betrieben werden, die nicht gepatcht werden können, beispielsweise, weil sie notwendige Fachverfahren sind, die bereits Jahrzehnte alt sind und keine Herstellerupdates mehr erhalten. Entsprechende veraltete Systeme (Betriebssysteme oder auch Programme) sollten sauber vom restlichen Netzwerk getrennt sein und möglichst keinen Kontakt zu externen Systemen besitzen. Hierzu hat das BSI Empfehlungen insbesondere in industriellen Steuerungs- und Automatisierungssystemen bereitgestellt [5].

3.4 Zugriffe auf Ransomware-C2 Server überwachen

Indem Zugriffe aus dem eigenen Netz auf bekannte Ransomware Command & Control (C2) Server überwacht oder im besten Fall sogar blockiert werden, kann man sofort über kompromittierte Systeme alarmiert werden. Einige Ransomwarevarianten benötigen darüber hinaus eine Verbindung zu C2 Servern, bevor die Daten verschlüsselt werden können. In diesen Fällen kann durch eine Verbindungsüberwachung / -beschränkung sogar die Verschlüsselung der Daten unterbunden werden.

Das Projekt „abuse.ch“ [6] der University of Applied Sciences, Schweiz, bietet hierzu Informationen zu aktiven C2-Servern, und auch zu kompromittierten Seiten, über welche schadhafte Dokumente verbreitet werden.

Möglich ist beispielsweise die Nutzung von Filterung über DNS. Idealerweise würde diese selbst betrieben werden, falls dies aber aus Ressourcengründen nicht möglich ist, könnten frei verfügbare DNS-Server mit Malwarefilterung genutzt werden. Somit würde zumindest der Zugriff auf bekannte maliziöse Webseiten blockiert werden.

4 Ausführbarkeit von Schadprogrammen einschränken (Client Einstellungen)

Trotz aller Maßnahmen werden Schadprogramme regelmäßig die Systeme erreichen. Daher sollte zusätzlich möglichst verhindert werden, dass diese auf den Systemen ausgeführt werden können. Die hier möglichen Maßnahmen hängen von dem jeweiligen Geräte-Typ, Betriebssystem und den eingesetzten Versionen ab.

4.1 Software-Updates

Um generell vor Infektionen durch die Ausnutzung bereits behobener Sicherheitslücken geschützt zu sein, sollten Updates unverzüglich nach der Bereitstellung durch den jeweiligen Softwarehersteller getestet und auch in die IT-Systeme - idealerweise über zentrale Softwareverteilung - eingespielt werden.

Wenn der Betrieb der IT-Systeme durch einen externen Dienstleister erfolgt, sind SLAs ggf. gestaffelt nach Kritikalität der Updates zu vereinbaren.

4.2 Deaktivieren oder Beschränken von Scripting Umgebungen und Makros

Auf Windows-Systemen sind viele der aktuellen initialen Schadprogramme auf PowerShell angewiesen, um ihr schadhaftes Potential entfalten zu können. Schränkt man die PowerShell entsprechend ein, ist eine Ausführung des eigentlichen Schadcodes oft eingeschränkt oder gar nicht mehr möglich.
Bei der Umsetzung der Maßnahmen sollte jedoch eingehend geprüft werden, welche Auswirkungen diese auf den regulären Betrieb haben.

Möglich ist es etwa den „ConstrainedLanguage Mode“ bei PowerShell zu aktivieren. Hierbei sind bestimmte Befehle und Funktionen gesperrt. Allerdings kann dieser Modus ggf. umgangen werden.
Weiterhin kann über eine Firewall der Internetzugriff für PowerShell blockiert werden. Dies schränkt viele Schadprogramme ein, weil diese oftmals weitere Module oder zusätzliche Schadprogramme nachladen.
Neben der Beschränkung sollte für die PowerShell auch das Logging aller Befehle (via GPO) aktiviert werden, um Aktionen von Angreifern nach Möglichkeit im Nachhinein nachvollziehen zu können.

Daneben werden auch verschiedene andere Scripting Umgebungen und Makros genutzt. Daher kann sinnvoll sein:

- Schutz vor Office-Makros mittels Gruppenrichtlinie, etwa Deaktivierung von Makros, sehr restriktive vertrauenswürdige Orte für Makros im AD konfigurieren oder nur die Ausführung von signierten Makros erlauben. Grundsätzlich sollten Makros, die in einer Institution genutzt werden, digital signiert sein und nur die Ausführung von Makros mit festgelegten digitalen Signaturen erlaubt werden.
- Ausführung von Skripten (z. B. *.bat, *.cmd, *.cs, *.reg, *.vbs, *.js) (temporär) verhindern, etwa über Gruppenrichtlinien für Softwareeinschränkungen.
- Grundsätzlich die Deaktivierung von Windows Script Host (WSH) über GPO.

4.3 Anwendungskontrolle

Ein Großteil aller Infektionen könnte verhindert werden, wenn die Ausführung und Installation unerwünschter Software grundsätzlich unterbunden wird. Dazu gibt es eine ganze Reihe an Maßnahmen. Eine der wichtigsten dabei ist die sogenannte Anwendungskontrolle "Application Whitelisting". Dieses lässt eine Ausführung nur von freigegeben Programmen zu. Da die Verwaltung solcher Erlaubtlisten sehr aufwendig ist, können stattdessen in einem ersten Schritt auch nur Verzeichnisregeln eingesetzt werden. Dabei wird die Ausführung von Programmen nur aus bestimmten Verzeichnissen (z. B. C:\Windows,

C:\Programme) erlaubt. Hierbei ist es wichtig, dem Nutzer die Schreibrechte auf diese Verzeichnisse zu entziehen, damit dieser, bzw. die Ransomware unter Verwendung seines Kontos, keine ausführbaren Dateien in diese Verzeichnisse kopieren kann. So würde zum Beispiel die Ausführung von Dateien im Verzeichnis *%TEMP%*, in welches Malware in der Regel beim Herunterladen abgelegt wird, unterbunden.

4.4 Virenschutz

Neue Versionen von Schadsoftware werden nur selten sofort über normale AV-Signaturen erkannt. Daher sollten bei professioneller Antivirensoftware konsequent alle verfügbaren Module genutzt werden. Die meisten Infektionen mit neuen Varianten von Ransomware werden durch die hostbasierten Intrusion Prevention (IPS)-Module und Cloud-Dienste der AV-Software verhindert. Dies ist auch der Grund, warum die Erkennung infizierter Dateien an Gateways sehr viel schlechter ist als bei den Viren-Schutzprogrammen für Endgeräte.

Häufig kann über zusätzliche AV-Module die Ausführung oder Verbreitung der Malware verhindert werden, indem diese verdächtiges und typisches Verhalten von Malware unterbindet. Wenn Malware eines bestimmten Typs z. B. immer die gleichen Verzeichnisse benutzt, um ihre Dateien zu speichern, kann die Ausführung von Dateien in diesen Verzeichnissen blockiert werden. Wer einen entsprechenden Supportvertrag abgeschlossen hat, sollte in jedem Fall bei seinem AV-Hersteller aktiv nach zusätzlichen Schutzmöglichkeiten und Konfigurationshinweisen nachfragen.

Da diese zusätzlichen Maßnahmen möglicherweise auch legitime Applikationen blockieren, empfiehlt es sich, neue bzw. verschärfte Regeln zuerst im „Log-only-Modus“ zu betreiben und während einer ausreichenden Testphase die Protokolldaten der AV-Software zu prüfen. Wenn legitime Applikationen von einer Regel berührt werden, können diese Anwendungen über Ausnahmeregeln von der Prüfung ausgenommen werden.

„Virenschutz“ hat sich im Sprachgebrauch eingebürgert, ist aber eigentlich keine geeignete Bezeichnung mehr für das in einer Enterprise-Umgebung benötigte Produktportfolio. Unter „Virenschutz“ muss in der Praxis immer eine vollständige IT-Sicherheitsarchitektur verstanden werden, die Endgeräte, Server, Gateways, physische und virtuelle Systeme sowie spezielle Anwendungen wie Webserver, E-Mail und Datenbanken umfasst.

Da nicht nur Windows-Systeme erfolgreich angegriffen werden, sollte unabhängig vom Betriebssystem geprüft werden, ob professionelle Viren-Schutzprogramme für den Enterprise-Bereich in Unternehmen und Behörden eingesetzt werden sollten. Enterprise-Produkte bieten oftmals erweiterte Konfigurationsmöglichkeiten und die Möglichkeit zur zentralen Administration. Unabhängig von Signaturupdates sollte immer die neueste Programmversion eingesetzt werden, da neue und verbesserte Erkennungsverfahren häufig nur in die aktuelle Version integriert werden

Sollten entsprechende Virenschutz-Lösungen Auffälligkeiten feststellen, muss diesen Meldungen unbedingt nachgegangen werden.

4.5 Behandlung von E-Mails

Viele E-Mails werden heutzutage als sogenannte HTML-E-Mails versendet, da diese eine „ansprechende Optik“ haben können. Allerdings können hierdurch auch Phishing-E-Mails als „vertrauenswürdig“ erscheinen, da verdächtige Inhalte sich einfacher verschleiern lassen. Daher sollte die Darstellung von E-Mails als sog. Textdarstellung (oft als "Nur-Text" bzw. "reiner Text" bezeichnet im Gegensatz zur Darstellung als "HTML-Mail") voreingestellt werden. Dadurch können etwa die Ziel-Webadressen nicht mehr verschleiert werden (In einer HTML-E-Mail könnte ein Link mit der Bezeichnung "www.bsi.de" z. B. in Wahrheit auf die Adresse "www.schadsoftwaredownload.tld" verweisen).

Auch sollte ein (automatisiertes) Nachladen von Dateien (Bildern, Skripte) in E-Mails verhindert werden.

4.6 Ausführung potentiell gefährlicher Inhalte in gekapselten Umgebungen

Eine weitere Schutzschicht kann die Ausführung potentiell gefährlicher Inhalte in gekapselten Umgebungen, insbesondere (Mirco-) VMs, sein. Dabei wird eine temporäre Arbeitsumgebung gestartet, welche regelmäßig wieder gelöscht oder zurückgesetzt wird. Wenn Dokumente und Dateien aus unsicheren Quellen in einer virtuellen Umgebung (VM) geöffnet werden, müsste entsprechende Schadsoftware aus dieser VM ausbrechen, um das eigentliche System zu infizieren. Entsprechende (Micro-) VMs können beispielsweise auch das Öffnen Links aus E-Mails abdecken. Selbstverständlich müssen auch entsprechende Lösungen, welche (Micro-) Virtualisierung anbieten aktuell gehalten werden. Zum einen können Betriebssystem-Updates zu Problemen führen, zum anderen kann nur so verhindert werden, dass Schadprogramme aus der VM ausbrechen können.

5 Bereiten Sie sich auf einen Vorfall vor

Trotz aller Maßnahmen ist es möglich, dass es zu einem Ransomware-Vorfall kommt. Das kann für Organisationen verheerend sein, wenn Systeme nicht mehr verfügbar sind und Daten nie wiederhergestellt werden können. Maßnahmen zur Wiederherstellung können häufig mehrere Wochen oder gar Monate in Anspruch nehmen. Zusätzlich hat ein Sicherheitsvorfall oft Auswirkungen auf die Reputation der Organisation. Daher sollte das jeweilige Vorgehen intensiv mit allen Beteiligten geübt werden, wie bei einem Vorfall in der Organisation zu verfahren ist. Die hierbei eingeübten Vorgehensweisen und sich aus der Übung ergebenden Lektionen sollten dann in Playbooks münden. Aber auch umgekehrt sollte auf Basis der erstellten Playbooks regelmäßig geübt werden. Eine Übersicht von möglichen Maßnahmen hat das BSI im Dokument „Erste Hilfe bei einem schweren IT-Sicherheitsvorfall“ [7] veröffentlicht.

Übungen sind ein vielfältig einsetzbares Mittel. Schon einfache Planbesprechungen und Übungen können sensibilisieren und dazu beitragen, am grünen Tisch zu überprüfen, wie eine Institution mit einem Vorfall umgehen würde. Damit werden außerdem auch Anforderungen aus dem Notfallmanagement z.B. nach dem modernisierten BSI-Standard 200-4 oder allgemeiner aus dem Business Continuity Management (BCM, BSI-Standard 200-4 als Community-Draft 1.0) erfüllt. Hierfür hat das BSI auch entsprechende Hilfsmittel bereitgestellt [8].

Bei entsprechenden Planbesprechungen und Übungen sollten insbesondere unterschiedliche Ausmaße der Kompromittierung (einzelne Systeme, einzelne Standorte oder schlicht „alle Systeme“) durchgespielt werden. Die folgenden Punkte sollten bedacht werden:

- Welche Geschäftsprozesse sind für die jeweilige Institution kritisch? Welche Systeme sind für den Geschäftsbetrieb zwingend notwendig und wie würde man diese nach einer Kompromittierung wiederherstellen?
- Wie wird zu dem Vorfall intern und extern kommuniziert? Es ist wichtig, dass die richtigen Informationen die richtigen Stakeholder zeitnah erreicht. Beachten Sie dabei auch nötige rechtliche Meldepflichten. Über welche Mittel oder Systeme werden diese informiert?
- Halten Sie eine Liste mit Dienstleistern für solche Notfälle bereit, beispielsweise zur Wiederherstellung oder forensischen Analyse ihrer IT-Systeme.
- Planen Sie, wie auf eine Erpressungsforderung reagiert werden sollte und welche Risiken bestehen, wenn Unternehmensdaten veröffentlicht werden.
- Stellen Sie sicher, dass auch bei Verschlüsselung von Daten Zugriff auf die Reaktions-Pläne und in diesem Zusammenhang zwingend notwendige Daten besteht. Hierzu kann es nötig sein, dass entsprechende Dokumente, Kontaktdaten und Passwörter in ausgedruckter Form vorliegen.
- Denken Sie daran, dass Aufsichtsbehörden eine unmittelbare Prüfung zur Kontrolle der technischen und organisatorischen Maßnahmen in Betracht ziehen können. Bereiten Sie sich im Rahmen der zu übenden Maßnahmen darauf vor und stellen Sie sicher, dass alle Unterlagen in ausgedruckter Form vorliegen und die Beschäftigten, welche mit Datenschutz-Themen vertraut sind, als Ansprechpartner zur Verfügung stehen.
- Auch das Wiederaufsetzen der verschiedenen Systeme sollte nicht nur theoretisch durchgespielt, sondern auch praktisch geübt werden. Dabei können die folgenden Fragen beantwortet werden:
  - Welche Prozesse und Reihenfolgen gibt es beim Wiederherstellen von Servern und Daten aus den Backup-Lösungen?
  - Wie lang nimmt das Wiederherstellen und Neukonfigurieren der zwingend nötigen Geräte in Anspruch?

- Wie wird vorgegangen, wenn lokale Systeme und Backups nicht mehr verwendbar sind und komplett aus Offline-Backups wiederhergestellt werden müssen? Was ist, wenn dann die Offline-Backups nicht mehr nutzbar sind?
- Wie werden virtuelle Umgebungen und physische Server neu aufgebaut?
  - Werden neue Systeme benötigt?
  - Wie viele neue Systeme sind notwendig?
  - Wie kommen Sie an neue physische Systeme? Können die üblichen Lieferanten schnell genug liefern oder haben Sie ggf. eigene Vorsorge getroffen (eigene Lagerhaltung)?
- Wie werden kritische Geschäftsprozesse aufrechterhalten?
- Welches Personal und welche Fähigkeiten werden wo in welcher Funktion benötigt?
- Wer kontrolliert die entsprechende Leak Seite um zeitnah auf einen Datenabfluss reagieren zu können?

Zusätzliche Orientierung bieten die weiteren Dokumente des BSI, wie etwa das Erste-Hilfe-Dokument [7].

Nach einem Vorfall sollte der Reaktions-Plan überarbeitet werden um erkannte Lektionen einfließen zu lassen. Dabei sollte im Besonderen Wert daraufgelegt werden, wie gleiche oder ähnliche Fälle künftig verhindert werden können.

Die Erkenntnisse sollten in geeigneten Erfahrungskreisen wie beispielsweisen Verbänden, UP KRITIS oder Allianz für Cybersicherheit (ACS) in geeigneter Weise geteilt werden. Durch einen gegenseitigen Austausch können alle Teilnehmenden derartiger Einrichtungen profitieren.

6 Weitergehende Schutzmaßnahmen

Weiterhin können folgende Punkte sinnvoll sein, um die Reaktion auf einen Vorfall zu verbessern, die Betroffenheit einzuschränken oder Schwachstellen zu erkennen:

6.1 Zentrales Logging

Wenn es zu einem Vorfall kommt, hilft die Auswertung von Logdaten dabei, dessen Ausmaß und die Infektionsquelle festzustellen. Mit der Auswertung von zuvor erfassten Logdaten können infizierte Systeme im Netzwerk identifiziert und idealerweise der initiale Infektionsweg nachvollzogen werden. Unternehmen sollten daher bereits im Vorfeld eine gut geplante Logging Policy etabliert haben und sicherstellen, dass die Logs auch regelmäßig erzeugt und mittels zentraler Logserver manipulationssicher gespeichert werden. Existiert noch keine Logging Policy im Unternehmen oder in der Behörde, dann sollte dies umgehend nachgeholt werden.

Die zentrale Sammlung kann etwa Bordmittel des Windows-Betriebssystems in Verbindung mit dem Windows Event Collector [9] oder durch Zusatzsoftware (Agenten) erfolgen.

Grundsätzlich müssen die Logs regelmäßig auf Auffälligkeiten überprüft werden. So gibt es Schadsoftware, welche mittels Brute-Force versucht sich auf Netzwerklaufwerke zu verbinden und sich hierüber zu verbreiten. Dies kann bei aktivem Monitoring der Logs bereits in einem frühen Stadium erkannt werden und so weitere Schäden verhindert werden. Ein automatisiertes, ständiges Monitoring der Logs kann durch ein SIEM in Echtzeit mit sofortiger Alarmierung erfolgen.

Insbesondere die Logs der Virenschutzsoftware auf Client-Systemen sollten zentral ausgewertet werden, um frühzeitig auf Angriffsversuche reagieren zu können. Weitere Empfehlungen zu Logging insbesondere bei Windows 10 hat das BSI unter [10] und [11] veröffentlicht. Wichtige Logdaten bei Servern sind beispielsweise E-Mail-Verkehr, An-/ Abmeldungen auf Systemen sowie entsprechende fehlgeschlagene Versuche, Remote-Verbindungen, Zugriff auf Daten, Zugriff auf Webseiten.

Dies jeweiligen Logdaten sowie die jeweilige Dauer der Speicherung müssen datenschutzkonform ausgewählt und verarbeitet geprüft werden.

6.1.1 HTTP-Proxy-Log

Beim Einsatz eines zentralen HTTP-Proxys empfiehlt das BSI, dass neben den reinen Verbindungsinformationen auch Referer, User-Agent und die Anzahl gesendeter Bytes mitgeloggt werden.

6.1.2 DNS-Logs

DNS-Logs bzw. passive DNS-Aufzeichnungen sind sehr hilfreich, wenn es darum geht festzustellen, ob und wann ein bestimmter Domainname aus dem Netzwerk der Institution aufgelöst wurde und zu welcher IP-Adresse dieser auflöste. Es ist daher ratsam entsprechende DNS-Anfragen zu loggen.

6.1.3 Sysmon

System Monitor (Sysmon) [12] ist ein Windows-Systemdienst und -Gerätetreiber, der nach der Installation auf einem System über Systemneustarts hinweg resident bleibt, um die Systemaktivität zu überwachen und im Windows-Ereignisprotokoll zu protokollieren. Sysmon erweitert dabei die bereits im Betriebssystem vorhandene Ereignisprotokollierung um zusätzliche Informationen. Es bietet beispielsweise detaillierte Informationen zu Prozesserstellungen, Netzwerkverbindungen und Änderungen an der Dateierstellungszeit.

Zur Konfiguration kann sich beispielsweise an [13] und [14] orientiert werden.

6.2 Systeme härten

Mit dem Projekt SiSyPHuS Win10 (Studie zu Systemintegrität, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10) lässt das BSI Sicherheitsanalysen der sicherheitskritischen Funktionen in Windows 10 durchführen sowie darauf aufbauend passende Härtungsempfehlungen erstellen [15]. Dabei hat das BSI beispielsweise Empfehlung zur Härtung von Windows 10 mit Bordmitteln [16] bereitgestellt.

6.3 Netzwerke segmentieren

Eine saubere Netzsegmentierung hilft Schäden zu begrenzen, da die Ransomware damit nur die Systeme in unmittelbarer Nachbarschaft erreichen kann. Hierbei ist insbesondere auch die sichere Verwendung von Administrator Accounts notwendig, da ansonsten ein zentraler Bestandteil des Sicherheitskonzepts untergraben wird. Die Einschränkung von Client zu Client-Verbindungen kann die Ausbreitung von Angriffen deutlich verlangsamen.

Durch eine geeignete bedarfsgerechte Konzeption des Active Directories kann das Risiko eines übergreifenden Vorfalls deutlich gesenkt werden. Durch die Unterteilung in verschiedene Ebenen mit Zugriffseinschränkungen kann eine Ausweitung von Rechten innerhalb eines Netzes verhindert werden. Durch Active Directories mit unterschiedlichen sog. Forests kann eine Ausbreitung von Malware über verschiedene Organisationseinheiten, etwa ein Standort oder Geschäftssegment hinaus, begrenzt werden. Diese Aufgabe erfolgreich korrekt umzusetzen ist von enormer Bedeutung, jedoch nicht trivial.

6.4 Erkennung von Ransomwareangriffen auf Fileservern

Mit dem Ressourcen-Manager für Datei-Server (File Server Ressource Manager) ist es möglich eine Dateigruppe mit der Endung *.* zu erstellen und eine Liste mit Ausnahmen zuzulassen (z. B. *.docx, *.xlsx, *.txt usw.). Damit wäre es, mit einer entsprechenden Dateiprüfungsregel möglich, das Erstellen von Dateien mit anderen Endungen als die in der Liste der Ausnahmen aufgezählten, zu verhindern bzw. zu erkennen. Mit Hilfe der Möglichkeit zur Erzeugung von Ereignisprotokolleinträgen, könnte auch durch Verknüpfung solcher Ereigniseinträge mit entsprechenden Aufgaben ggfs. Maßnahmen - Skripte können aufgerufen werden - ergriffen werden, etwa Alarmierung, Sperrung von Accounts, etc.

Auch könnten sog. „Canary Files“ genutzt werden, also Shares und Dateien, auf welche üblicherweise nicht zugegriffen werden. Sollten hier Zugriffe erfolgen könnten diese verdächtige Aktionen sein, welche untersucht werden sollten.

6.5 Anomalie-Detektion

Durch Anomalie-Detektion im Netzwerk ist es möglich zeitnah Datenabfluss zu erkennen. Hierfür ist es nötig den regulären Traffic (Baseline) sehr gut zu kennen. Wenn man diese Baseline hat, ist es möglich, künftigen Traffic mit sinnvoll gewählten Schwellwerten zu prüfen und mögliche Abweichungen zu erkennen und geeignete Maßnahmen zu ergreifen.

6.6 Schwachstellenscan und Penetrationstest

Als ergänzende Maßnahme können IT-Systeme mit einem Penetrationstest und regelmäßigen Schwachstellen-Scans darauf geprüft werden, ob die Härtungs- und Absicherungsmaßnahmen, beispielsweise gegen die Ausbreitung der Ransomware oder das Übergreifen auf Backup-Medien, geeignet umgesetzt worden sind. Bei solchen regelmäßigen Schwachstellen-Scans soll insbesondere darauf geprüft werden, ob Aktualisierungen für Betriebssysteme, Browser und andere Anwendungen laufend eingespielt werden.

Eine entsprechende Überprüfung kann auch durch ein externes Beratungsunternehmen durchgeführt werden. Auf den Webseiten der ACS finden Sie eine Übersicht der durch das BSI zertifizierten IT-Sicherheitsdienstleister für IS-Revision und IS-Beratung sowie Penetrationstests.

7 Nutzen-Aufwand-Abschätzung der vorgestellten Maßnahmen

Die folgenden Einschätzungen sind sehr allgemein und können für die jeweilige Behörde oder das Unternehmen deutlich abweichen. Dennoch kann der hier dargestellte Vergleich erste Hinweise geben, welche Themen prioritär angegangen werden sollten. Maßnahmen, welche als kurzfristig besonders hilfreich angesehen werden (Quick-Wins), sind gesondert markiert. Aufgrund der Subjektivität der Einschätzungen kann auch bei gleichen Nutzen-Aufwand-Einträgen nicht darauf geschlossen werden, dass beide Quick-Wins sein müssen oder nicht.

Tabelle 2 Nutzen-Aufwand-Abschätzung der möglichen Maßnahmen

Maßnahme	Nutzen ++ sehr gut -- sehr eingeschränkt	Aufwand ++ sehr einfach -- sehr schwer	Quick-Wins
Backups	++	0	x
Server: Umgang mit E-Mails	+	0	
Server: Aktives Schwachstellenmanagement	++	0	x
Freigabe nur notwendiger Dienste und Ports	++	+	x
Remote-Zugänge absichern	++	+	
Sicherer Umgang mit Administrator Accounts	+	++	
Veraltete Systeme isolieren	++	0	
Zugriffe auf Ransomware-C2 Server überwachen	0	0	
Client: Software-Updates	0	++	
Deaktivieren oder Beschränken von Scripting Umgebungen und Makros	++	0	x
Anwendungskontrolle	++	-	
Virenschutz	-	+	
Client: Behandlung von E-Mails	-	++	
Ausführung potentiell gefährlicher Inhalte in gekapselten Umgebungen	++	-	
Bereiten Sie sich auf einen Vorfall vor	+	+	x
Zentrales Logging	+	-	
Systeme härten	0	--	
Netzwerke segmentieren	++	--	
Erkennung von Ransomwareangriffen auf Fileservern	-	-	
Anomalie-Detektion	0	--	
Schwachstellenscan und Penetrationstest	0	+	

8 Literaturverzeichnis

1. **BSI.** Ransomware: Management Fortschrittliche Angriffe. [Online] 2021. März 13. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Managementabstract-Angriffe.html.

2. **Springer Gabler.** Gabler Wirtschaftslexikon - Höhere Gewalt - Definition. [Online] 31. März 2020. [Zitat vom: 25. November 2021.] https://wirtschaftslexikon.gabler.de/definition/hoehere-gewalt-32096/version-376045.

3. **BSI.** CON.3: Datensicherungskonzept (Edition 2021). [Online] 1. Februar 2021. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/03_CON_Konzepte_und_Vorgehensweisen/CON_3_Datensicherungskonzept_Edition_2021.pdf.

4. —. Maßnahmen zum Schutz vor Emotet und gefährlichen E-Mails im Allgemeinen. [Online] 2020. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/Malware/Emotet/emotet_node.html.

5. —. Umgang mit "End of Support" in industriellen Steuerungs- und Automatisierungssystemen. [Online] 10. Oktober 2021. https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_145.pdf.

6. **abuse.ch.** abuse.ch - Fighting malware and botnets. [Online] 2021. https://www.abuse.ch.

7. **BSI.** Ransomware: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall Version 1.1. [Online] 28. Januar 2020. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.html.

8. —. BSI-Standard 200-4: Hilfsmittel. [Online] 2021. [Zitat vom: 26. Novemer 2021.] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/BSI-Standard-200-4_Hilfsmittel/BSI_Standard_200_4_Hilfsmittel_node.html.

9. **Microsoft.** Windows-Ereignissammlung. [Online] https://docs.microsoft.com/de-de/windows/win32/wec/windows-event-collector.

10. **BSI.** Configuration Recommendations for Windows 10 Logging. [Online] 21. April 2021. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Cyber-Security/SiSyPHuS/AP10/Logging_Configuration_Guideline.pdf.

11. —. Empfehlung zur Konfiguration der Protokollierung in Windows 10. [Online] 2020. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Empfehlung_zur_Konfiguration_der_Protokollierung_Win_10.html.

12. **Microsoft.** Sysmon. [Online] https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon.

13. **SwiftOnSecurity.** sysmon-config | A Sysmon configuration file for everybody to fork. [Online] https://github.com/SwiftOnSecurity/sysmon-config.

14. **olafhartong.** sysmon-modular | A Sysmon configuration repository for everybody to customise. [Online] https://github.com/olafhartong/sysmon-modular.

15. **BSI.** SiSyPHuS Win10: Studie zu Systemaufbau, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10. [Online] https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/SiSyPHuS_Win10/SiSyPHuS_node.html.

16. —. SiSyPHuS Win10: Empfehlung zur Härtung von Windows 10 mit Bordmitteln. [Online] https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/SiSyPHuS_Win10/AP11/SiSyPHuS_AP11_node.html.