Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Erste Hilfe bei einem schweren IT-Sicherheitsvorfall

Arbeitspapier – Version 1.2

Änderungshistorie

Version	*Datum*	*Beschreibung*
1.0	17.12.2019	Erste Veröffentlichung
1.1	28.01.2020	Neues Kapitel „Lösegeld bezahlen?“ Kleinere Änderungen Anpassungen an Barrierefreiheit
1.2	07.10.2022	Kleinere Änderungen Neues Kapitel „Daten-Leak“

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel: +49 22899 9582-0
E-Mail: certbund@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

1 Kurzfassung

Organisation

- Bewahren Sie Ruhe und handeln Sie nicht übereilt.
- Richten Sie einen Krisenstab (oder eine Projektgruppe) ein.
- Klären Sie regelmäßig folgende Fragen:
  - Wer macht was bis wann?
  - Welche Tagesaufgaben können für die Bewältigung des Vorfalls liegen gelassen werden?
  - Wer trifft die relevanten Entscheidungen?
  - Sollen Systeme schnell wieder aufgesetzt werden oder Spuren gesichert werden?
  - Wer kommuniziert was wann an wen?
  - Wollen Sie Anzeige erstatten?
- Denken Sie an Meldepflichten.
- Holen Sie sich bei Bedarf frühzeitig externe Unterstützung.
- Kurzfristig für den Notbetrieb wichtige Daten können sich auch an ggf. abgesetzten Außenstellen oder auf Systemen von Mitarbeitern im Urlaub befinden, welche (noch) nicht betroffen sind.
- Mit einem Abfluss von Daten ist zu rechnen.

Technik

- Oberste Regel: Keinesfalls darf eine Anmeldung mit privilegierten Nutzerkonten (Administratorkonten) auf einem potenziell infizierten System erfolgen, während das System sich noch im internen produktiven Netzwerk befindet oder mit dem Internet verbunden ist!
- Potenziell infizierte Systeme sollten umgehend vom Netzwerk isoliert werden, um eine weitere Ausbreitung der Schadsoftware im Netz durch Seitwärtsbewegungen (Lateral Movement) zu verhindern. Dazu das Netzwerkkabel ziehen. Gerät nicht herunterfahren oder ausschalten. Gegebenenfalls forensische Sicherung inkl. Speicherabbild für spätere Analysen (eigene, durch Dienstleister oder Strafverfolgungsbehörden) erstellen.
- Die Schadprogramme nehmen teilweise tiefgreifende (sicherheitsrelevante) Änderungen am infizierten lokalen System vor, die nicht einfach rückgängig gemacht werden können. Das BSI empfiehlt daher grundsätzlich, infizierte lokale Systeme als vollständig kompromittiert zu betrachten und neu aufzusetzen.
- Fortschrittliche Schadsoftware-Varianten können sich mit ausgespähten Zugangsdaten für Benutzerkonten (ggf. mit administrativen Rechten) lateral im Netzwerk ausbreiten. Beachten Sie die Problematik eines „Golden Tickets“ und Kompromittierungen von Domaincontrollern und Serversystemen (Active Directory und alle domain-joined Systeme neu aufsetzen). Sollte das nicht schnell möglich sein, muss das Passwort des eingebauten Key Distribution Service Accounts (KRBTGT) zweimal zurückgesetzt werden. Dies invalidiert alle Golden Tickets welche mit dem zuvor gestohlenen KRBTGT-Hash und allen anderen Kerberos Tickets erzeugt wurden.[1]
- Alle auf betroffenen Systemen gespeicherten bzw. nach der Infektion eingegebenen Zugangsdaten sollten als kompromittiert betrachtet und die Passwörter geändert werden. Dies umfasst u. a. Webbrowser, E-Mail-Clients, RDP/VNC-Verbindungen sowie andere Anwendungen wie PuTTY, FileZilla, WinSCP, etc.
- Blockieren Sie jede nicht unbedingt benötigte Remote-Verbindung, beobachten Sie den Netzwerkverkehr und lassen Sie Antiviren-Scans laufen um weitere Infektionen und Täterzugriffe auszuschließen.
- Prüfen Sie, ob Sie saubere, nicht kompromittierte Backups haben.

[1] http://cert.europa.eu/static/WhitePapers/UPDATED%20-%20CERT-EU_Security_Whitepaper_2014-007_Kerberos_Golden_Ticket_Protection_v1_4.pdf – insb. Kap. 3.2

- Im Fall einer bereits erfolgten Verschlüsselung sollten Sie grundsätzlich nicht auf die Erpressung eingehen und kein Lösegeld bezahlen. Stattdessen sollten die Daten in ein sauberes Netzwerk aus Backups zurückgespielt werden.
- Eine Persistenz von Schadsoftware im BIOS oder gar der Hardware ist sehr selten und wird bislang nicht von breit verteilter Schadsoftware angewandt.
- Um einen zukünftigen weiteren Zugriff der Täter auf das interne Netzwerk und eine erneute Ausbreitung von Schadsoftware auszuschließen, sollte im Fall einer Kompromittierung des AD das Netz unbedingt komplett neu aufgebaut werden. Dies kann nach einer schnellen Bereinigung u.U. auch langfristig nach Sicherstellung der Betriebsfähigkeit erfolgen.

2 Über dieses Dokument

Dieses Dokument dient als Notfalldokument für IT-Sicherheitsbeauftrage, CISOs und Systemadministratoren von KMUs und kleineren Behörden für den Fall eines schweren IT-Sicherheitsvorfalls. Dies kann etwa die Infektion von einer Reihe an Systemen mit einer fortschrittlichen Schadsoftware wie Emotet oder Trickbot oder eine bereits durchgeführte Verschlüsselung mit Ransomware sein. Im Schwerpunkt geht dieses Papier auf die Kombination fortschrittlicher Schadsoftware und Ransomware ein, welche ein gesamtes Netz übernehmen und verschlüsseln kann.

Wir werden dieses Dokument unregelmäßig mit aktuellen Erfahrungen ergänzen. Bitte prüfen Sie dies in geeigneten Abständen auf der Webseite des BSI.

Anspruch und Ziel des vorliegenden Arbeitspapiers ist eine erste systematische Hilfestellung bei einem schweren IT-Sicherheitsvorfall. Das Arbeitspapier kann nicht auf unternehmensspezifische Besonderheiten eingehen, und es kann auch keine individuellen Beratungsleistungen durch Experten (Techniker, Juristen etc.) ersetzen

Kapitel 3 richtet sich an die Managementebene, Kapitel 4 an operativ arbeitende Personen.

Wir danken allen Betroffenen und Helfern die uns Rückmeldungen geliefert haben dieses Dokument hilfreicher für den Ernstfall zu machen.

3 Incident Management – Organisatorische Maßnahmen

In diesem Kapitel werden generelle Maßnahmen und Empfehlungen für das Incident Management im Rahmen eines schweren IT-Sicherheitsvorfalls vorgestellt.

Stellen Sie sich drauf ein, dass Sie ggf. viele Tage lang (große) Teile Ihrer Dienstleistung nicht erbringen können oder Ihre Produktionsanlagen stillstehen (Erfahrungswerte bei vollständiger Kompromittierung: 2-4 Wochen). Richten Sie ein geeignetes Krisenmanagement (Kapitel 3.2) ein, das neben den technischen Wiederherstellungsaspekten (Kapitel 4) besonders die Kommunikation mit Ihren Stakeholdern, den Behörden und ggf. der Presse adressiert (Krisenkommunikation, Kapitel 3.3).

3.1 Vorfallsbewältigung als Projekt

Sollten Sie noch keine Erfahrung in der Bewältigung schwerer IT-Sicherheitsvorfälle haben, kann es sinnvoll sein, die Vorfallsbewältigung als Projekt aufzufassen und diese mit den Mitteln des Projektmanagements anzugehen.

Versuchen Sie die in Kapitel 3.2 genannten Maßnahmen des Krisenmanagements im Projektteam zu adressieren und umzusetzen.

Der Ablauf der Vorfallsbewältigung kann grob in drei Phasen eingeteilt werden.

- Phase 1: Analyse
  - Identifikation betroffener Systeme
  - Verhinderung weiterer Infektion und Verschlüsselung
  - Schadensfeststellung
  - Analyse der Schadprogramme
- Phase 2: Übergangsbetrieb
  - Verhinderung weiterer Infektion und Verschlüsselung
  - Blockierung der Täterzugänge
  - Intensives Monitoring des Netzes
- Phase 3: Bereinigung
  - Konzeption / Umsetzung / Neustart
  - Weitere Sicherheitsmaßnahmen (neues Sicherheitskonzept)

Der Fokus dieses Dokumentes liegt darauf, Betroffene bei einem guten Einstieg in Phase 1 zu unterstützen.

3.2 Krisenstab

Wie bereits in der Vorbemerkung zu Kapitel 3 dargestellt kann der Vorfall Auswirkung auf Ihre Dienstleistungen und Produkte haben. Größere IT-Sicherheitsvorfälle benötigen neben operativ-technischen Bewältigungsmechanismen auch administrativ-organisatorische Maßnhamen. Diese werden im Themenkomplex des IT-Krisenmanagements zusammengefasst.

Hauptmerkmale der administrativ-organisatorischen Bewältigungsmechanismen sind:

- eine ebenen-übergreifende und interdisziplinäre Sichtweise,
- die Behandlung strategischer Fragestellungen und Themenfelder,
- die Kenntnis kritischer Geschäftsprozesse und deren Bewertung auf Managementebene,
- die Steuerung der internen und externen Kommunikation und
- weitreichende Entscheidungs- und Handlungskompetenzen.

Diese Merkmale (Anforderungen) sollten jederzeit durch Ihr Projektteam erfüllt werden und erfordern eine fortlaufende Selbstkontrolle zur Aufrechterhaltung der administrativ-organisatorischen Ausrichtung.

Binden Sie daher frühzeitig relevante interne Stellen ein, zum Beispiel in Form eines Krisenstabes:

- Leitungsebene als Leiter des Krisenstabes (nach Möglichkeit jedoch nicht „den Kopf“ der Institution),
    - Damit der Krisenstab auch formal die Unterstützung der Geschäftsführung hat, der Kopf des Unternehmens als Gesicht nach außen aber auch nicht überlastet wird.
- IT-Leitung,
    - Als technischen Sachverstand für den Krisenstab, um operative Kräfte für die Arbeit freizuhalten.
- Juristen,
    - Fragen zu Haftung, Strafanzeige, weitere rechtliche Aspekte.
- Presse- und Öffentlichkeitsarbeit,
    - eine angemessene Krisenkommunikation nach innen und außen bewahrt die Reputation des Unternehmens, schützt Geschäftsbeziehungen und motiviert die Mitarbeiterinnen und Mitarbeiter
- Datenschutzbeauftragte sowie
    - Für datenschutzrechtliche Fragen das wie Logging.
- Personal- / Betriebsrat.
    - Wegen Zugriff auf Logdaten sowie personalrelevante Fragen wie Überstunden.

Mögliche Punkte einer Sitzung des Krisenstabes finden Sie im Anhang 6.4.

Planen Sie regelmäßige Beratungsphasen des Krisenstabes im Wechsel mit Arbeitsphasen.

Sie benötigen nicht für alle Rollen des Krisenmanagements Personal aus der IT-Abteilung! Projektmanager und Bürofachkräfte können die nun dringend benötigen IT-Spezialisten bei vielen organisatorischen, planerischen, kommunikationsrelevanten oder logistischen Aufgaben unterstützen und entlasten. Holen Sie sich bei Bedarf Unterstützung durch einen erfahrenen externen Krisenmanager ins Haus, der Sie bei der Bewältigung des Vorfalls begleitet.

Vermutlich müssen Sie kurzfristig das Active Directory (AD) bereinigen und mittel- bis langfristig neu aufsetzen. Prüfen Sie, ob an anderen Standorten oder in entfernten / separierten Unternehmensteilen nicht-betroffene ADs und (Teil-) Backups verfügbar sind. Richten Sie kurzfristig eine Projektgruppe ein, die - parallel zu Ihren Analysen und Eindämmungen - einen neuen Netzaufbau, insbesondere für kritische Geschäftsprozesse zur Aufrechterhaltung bzw. Wiederherstellung der Produktion, in einem segmentierten Bereich beginnt (ggf. mit externer Unterstützung).

Kümmern Sie sich um Ihre Mitarbeiterinnen und Kollegen, die zur Bewältigung der Lage Höchstleistungen erbringen. Sorgen Sie für Entlastungen (Getränke, Snacks, ggf. Taxinutzung, Hotel statt langer Heimfahrt). Achten Sie auf Anzeichen der Überlastung und lösen Sie sie geeignet aus der Krisensituation, damit sie den Kopf wieder frei bekommen und frische Energie tanken können ("Dienst- / Schichtplanung"). Beachten Sie, dass alles was Sie für Ihre Kollegen tun, kostengünstiger ist als ein verlängeter Produktionsausfall durch Fehler oder Überlastung!

Denken Sie aber auch an Mitarbeiter, welche durch den Ausfall von IT wenig bis gar nicht mehr arbeiten können. Versuchen Sie für diese sinnvolle Arbeiten zu finden und hierüber einen Notbetrieb einzurichten. Diese Mitarbeiter könnten auch noch (ggf. entgegen der Unternehmensrichtlinien) lokal gespeicherte Daten und Arbeitshilfen haben. Mit einem Hinweis „wird nicht geahndet“ könnten Sie hier noch wertvolle Daten finden.

Stellen Sie kurzfristig eine zuverlässige Erreichbarkeit für interne und externe Kommunikation sicher. Dies umfasst sowohl Telefone, im Zweifel kurzfristig beschaffte Prepaid-Handys. Gleichermaßen sollten E-Mail-Adressen und falls nötig auch eine kurzfristig erstellte Übergangs-Webseite erstellt werden.

3.3 Kommunikation

Die interne und externe Kommunikation bei schweren IT-Sicherheitsvorfällen ist sowohl eines der wichtigsten Tools für die nach außen sichtbare Bewältigung des Vorfalls als auch eine der größten Herausforderungen.

Daher sollte diesem Themengebiet eine besondere Bedeutung zukommen.

Überlassen Sie die Kommunikation den Spezialisten!

Sofern Sie innerhalb der eigenen Institution geeignete Ressourcen (bspw. Unternehmenskommunikation) identifizieren können, gilt es diese zu einem frühest möglichen Zeitpunkt in den Krisenstab / das Projektteam einzubinden.

Sofern Sie keine geeigneten Ressourcen aus der eigenen Institution stellen können, ziehen Sie externe Kommunikationsspezialisten hinzu. Diese werden Ihnen nach einer Analyse der vorliegenden Situation geeignete Maßnahmen vorschlagen.

Stellen Sie die notwendige Kommunikationsinfrastruktur bereit!

Je nach Ausmaß des Sicherheitsvorfalls kann es sein, dass die vorhandene Kommunikationsinfrastruktur (PC mit Internet, (VoIP-)Telefonie) nicht mehr einsatzfähig ist. Stellen Sie daher rechtzeitig eine geeignete Ersatzinfrastruktur (Laptops mit mobilem Hotspot, Handys mit Headsets) für die mit der Kommunikation befassten Stellen bereit.

Stakeholder identifizieren und Sprachregelung abstimmen!

Für eine geeignete Krisenkommunikation müssen Sie wissen, wer der Empfänger Ihrer Informationen sein soll / muss. Die eigenen Mitarbeitenden, Kunden, Gesellschafter, Lieferanten, Regulatoren und die allgemeine Öffentlichkeit sind nur eine Auswahl an möglichen Stakeholdern Ihrer Institution.

Bei direkter Kommunikation mit den Stakeholdern können Sie auch auf speziellere Fragen eingehen. Übliche Sorgen sind beispielsweise, ob über möglicherweise bestehende VPN-Verbindungen die Gefahr auch für Dritte (z.B. Ihre Lieferanten oder Kunden) ausgeht.

Stimmen Sie innerhalb des Projektteams – unter Einbeziehung aller beteiligten Fachbereiche – eine Sprachregelung ab und kommunizieren Sie diese innerhalb der Institution um alle Beteiligten in ihrem Sinne reaktionsfähig aufzustellen.

Interne Kommunikation vor externer Kommunikation!

Denken Sie zuerst an die Information Ihrer Mitarbeitenden und unterrichten Sie zeitnah über die Hintergründe des Vorfalls, um Spekulationen zu vermeiden. Geben Sie Verhaltenshinweise zum Umgang mit den (sozialen) Medien und sensibilisieren Sie die Mitarbeitenden über die nun bevorstehenden Maßnahmen. Die Information kann etwa über gut sichtbare Aushänge, bestehende Chat-Gruppen oder die jeweilige Führungskraft erfolgen.

Senden Sie mindestens eine „we care"-Botschaft. Nichts zu sagen ist keine empfehlenswerte Option!

Prüfen Sie frühzeitig eine Medieninformation zur Erlangung der Informationshoheit und zur Vermeidung von Spekulationen. Es ist möglich, dass die interne Information der Mitarbeiter nach außen gelangt. In diesem Fall sollten Sie sprechfähig sein.

Nutzen Sie die vorhandenen und bekannten Medien (Webseiten, Soziale Medien, etc.) Ihrer Institution um die Informationen zielgruppengerecht zu steuern. Verzichten Sie auf grafische Highlights und dynamische Inhalte und liefern Sie barrierefreie, kurze, prägnante Informationen, die regelmäßig (mindestens alle 48 Stunden) aktualisiert werden. Gestalten Sie die Seite z.B. als „Tagebuch" indem Sie die neuen Inhalte mit Zeitstempel von oben nach unten ergänzen während die Inhalte der vergangenen Tage / Wochen weiter nach unten rutschen.

Informieren Sie zeitnah – unter Einbeziehung des Datenschutzes sowie der Personalvertretung – über eine potenzielle private Betroffenheit der Mitarbeitenden, wenn eine Nutzung der IT für private Zwecke erlaubt ist und auf infizierten Systemen eingegebene oder gespeicherte (Zugangs-) Daten abgeflossen sein könnten.

Eine Liste möglicher Beteiligter sowie von wichtigen Punkten für eine Pressemitteilung finden Sie im Anhang 6.2.

Bündeln Sie den Informationsfluss und nutzen Sie FAQs!

Die Kanäle, über die Sie Krisenkommunikation betreiben, sollten sorgsam gewählt werden. Beachten Sie bei der Auswahl die bekannten Informationskanäle (zentrale E-Mail-Adressen, Rufnummern, etc.) und planen sie den Informationsfluss so, dass

- ausgehende Informationen möglichst von einem zentralen Absender versendet werden, der keinen Rückschluss auf eine Person zulässt und über den sie auch Reaktionen / Rückfragen erwarten,
- jeder extern bekannte Informationskanal überwacht wird,
- das Personal welches Informationen von extern aufnehmen soll, entsprechend unterrichtet ist und in der Lage ist mit energischen Anrufern umzugehen,
- alle eingehenden Informationen an einer zentralen Stelle gebündelt werden können, damit sie schnell ein umfassendes Bild erlangen,
- wiederkehrende Fragen und relevante Botschaften der Institution in einem FAQ zusammengefasst und geeignet veröffentlicht werden.

Für „blame, name, shame“ und „bashing“ ist in der Krise kein Platz!

Die Krisenkommunikation sollte nicht dafür genutzt werden, um mit dem Finger auf vermeintliche Verursacher zu zeigen. Eine professionelle und lösungsorientierte Krisenkommunikation ist in einem schweren IT-Sicherheitsvorfall das Aushängeschild der Institution und ggf. die einzige Möglichkeit eine positive Wahrnehmung zu schaffen.

Daher gilt:

- keine Schuldzuweisungen!
- Nennung von (Firmen-) Namen dritter beteiligter Behörden und Unternehmen (z. B. IT-Dienstleister) nur nach Abstimmung!
- kooperative Zusammenarbeit zwischen allen Beteiligten mit dem gemeinsamen Ziel einer umfassenden Bewältigung herausheben!

Sagen Sie öffentlich sowie gegenüber ihren Mitarbeitenden jederzeit die Wahrheit!

Formulieren Sie gemeinsam mit Ihrem Pressesprecher eine Sprachregelung zum Vorfall und informieren Sie frühzeitig Ihre Mitarbeiter.

Zum Thema Krisenkommunikation hat das Bundesministerium des Inneren einen sehr ausführlichen Leitfaden veröffentlicht[2]. Dieser gibt weitere Anhaltspunkte zur Durchführung der Krisenkommunikation – sowohl akut als auch präventiv.

Unabhängig davon bestehen ggf. gesetzliche Meldepflichten, darauf geht das nachfolgende Kapitel 3.6 ein.

3.4 Kurzfristige Wiederherstellung der Arbeitsfähigkeit

Die Wiederherstellung der vollständigen Arbeitsfähigkeit erfordert regelmäßig das Neuaufsetzten des betroffenen Active Directories. Zur kurzfristigen Wiederherstellung einer Teilarbeitsfähigkeit bietet es sich an, jede Dienstleistung zunächst einer der folgenden vier Kategorien zuzuordnen.

2 https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/leitfaden-krisenkommunikation.html

„Nicht betroffen“

Dienstleistungen, die keines der betroffenen Systeme verwenden.

„Auslagerungsfähig“

Dienstleistungen, die betroffene Systeme verwenden, die aber auf ein anderes eigenes oder fremdes System ausgelagert werden können. Die Auslagerungsfähigkeit kann je nach Dienstleistungen aber insbesondere auch nach der Größe der Organisation, der Organisationsumwelt und der eigenen AD-Landschaft stark variieren. In diese Kategorie gehören Dienstleistungen, bei denen kurzfristig ein anderer Standort der Organisation oder eine andere Organisation innerhalb eines Organisationsverbunds (z.B. anderes Konzernunternehmen, benachbarte Kommune, Geschäftsstelle eines Verbands) die erforderliche IT-Ausstattung (neben Clients auch Server mit entsprechenden Fachverfahren) für die eigenen Beschäftigten zur Verfügung stellen kann.

„mit mobilem Equipment zumindest eingeschränkt Arbeitsfähig“

Dienstleistungen, die betroffene Systeme verwenden, aber auch mit mobilem, nicht betroffenen, Equipment („sauberer“ Laptop, mobiler Hotspot, Handy) zumindest eingeschränkt erbracht werden können. In Abgrenzung zu auslagerungsfähigen Dienstleistungen handelt es sich hier um die Bereiche, bei denen die eingesetzten Softwaresysteme entweder rein Clientseitig funktionieren oder die externe Serverkomponente über das Internet erreichbar ist.

„ohne Neuaufbau nicht Arbeitsfähig“

Dienstleistungen, bei denen die Arbeitsfähigkeit nicht nach den vorgenannten Kategorien besteht oder hergestellt werden kann.

In einem nächsten Schritt können dann unter den Dienstleistungen jeder Kategorie diejenigen identifiziert werden, die als funktionswichtig angesehen werden und deshalb priorisiert lauffähig gemacht werden müssen.

3.5 Schadensanalyse

Die Schadensbewältigung setzt eine genaue Schadensanalyse voraus. Zusätzlich zu den bei der Kategorisierung unter Kapitel 3.4 gewonnenen Erkenntnissen ist eine Übersicht über die vorhandenen Daten (nicht betroffene Systeme, Backups), sowie über die von externen Datenquellen zu erlangenden Daten zu erstellen.

Neben einer Bemessung des Schadens ist die Aufklärung der Schadensursache erforderlich. So kann sichergestellt werden, dass die für den Sicherheitsvorfall verantwortlichen Schwachstellen beseitigt werden können.

3.6 Meldepflichten

Denken Sie an etwaige Meldepflichten etwa nach DSGVO, BSIG und anderen Gesetzen gegenüber Regulatoren. Beachten Sie außerdem etwaige Verpflichtungen aus vertraglichen Vereinbarungen.

Bei DSGVO-Verstößen wie dem Abfluss personenbezogener Daten – was etwa bei Emotet-Infektionen durch das Ausspähen von E-Mails aus Outlook-Postfächern immer der Fall ist – ist außerdem die in Art. 33 DSGVO genannte Meldeverpflichtung gegenüber der zuständigen Aufsichtsbehörde (Landesdatenschutzbeauftragten) zwingend zu beachten. Eine Meldung hat i.d.R. innerhalb von 72 Stunden zu erfolgen. Daneben - was häufig übersehen wird - sind in besonders risikoträchtigen Fällen auch die konkret betroffenen natürlichen Personen - also diejenigen Personen, deren Daten abgeflossen sind (Mitarbeiter, Kunden, Newsletterempfänger, ...) - in nachvollziehbarer, verständlicher Art über die betroffenen Dateninhalte, das Missbrauchspotenzial sowie die eigenen ergriffenen Schutzmaßnahmen zu

informieren (Art. 34 DSGVO)[3]. Selbst wenn ein Angriff relativ früh entdeckt wird, ist die Wahrscheinlichkeit groß, dass bereits die Daten, an denen der Angreifer ein Interesse und auf die er Zugriff hat, abgeflossen sind. So leitet die Schadsoftware „Emotet“ automatisiert Kontaktbeziehungen und E-Mail-Inhalte von Outlook aus.

Sollte eine Kritische Infrastruktur nach BSIG betroffen sein ist unter Umständen auch hier eine Meldung unverzüglich notwendig (§ 8b Absatz 4 BSIG). Dies gilt ebenso für Anbieter digitaler Dienste (§ 8c Absatz 3 BSIG).

Auch aus den von Ihnen geschlossenen Verträgen können Pflichten zur Information Ihrer Vertragspartner bestehen.

Wenn Sie eine Cyber-Versicherung haben, informieren Sie diese frühzeitig. Häufig gibt Ihnen diese Vorgaben, was Sie tun können.

3.7 Externe Unterstützung

Oftmals besitzen betroffene Institutionen nicht genug interne Expertise oder Ressourcen für die erfolgreiche Bewältigung von schweren IT-Sicherheitsvorfällen. Für viele Betroffene ist es das erste Mal, dass sie mit einem schweren IT-Sicherheitsvorfall konfrontiert werden. **Wenden Sie sich daher frühzeitig an externe Experten, wenn Sie sich überfordert fühlen.**

Folgende Hinweise bezüglich externer Unterstützung gelten für Institutionen in Deutschland. In anderen Ländern sollten die entsprechenden lokalen Behörden kontaktiert werden.

IT-Sicherheitsdienstleister

Allgemein ist bei der Auswahl eines Forensik-Unternehmens zu beachten, dass die Unternehmen unterschiedliche Analyseschwerpunkte haben. Die Bandbreite des Knowhows reicht dabei von der Analyse netzwerkbasierter Angriffen bis hin zur Wiederherstellung von physisch zerstörten Festplatten. Qualifizierte Dienstleister sind darauf eingestellt schnell zu reagieren.

Der Unterstützungsbedarf muss bei der Anfrage möglichst klar beschrieben werden. Benötigen Sie Hilfe bei dem Bereinigen von Systemen und des ADs, soll der Einfallsvektor gefunden werden oder weitere betroffene Systeme? Ist Personal für den Wiederaufbau des Netzwerks erforderlich?

Das BSI arbeitet im Rahmen der Allianz für Cybersicherheit mit etablierten Unternehmen mit dem Schwerpunkt Computerforensik aus Deutschland zusammen. Daneben hat das BSI hat eine Liste qualifizierter APT-Response-Dienstleister veröffentlicht[4]. Auch bieten Vorfall-Experten[5] oder teilweise zertifizierte Dienstleister in den Bereichen IS-Revision und IS-Penetrationstest[6] entsprechende Unterstützung an.

Prüfen Sie auch, ob Sie ggf. über Rahmenverträge kurzfristig Unterstützung beauftragen können.

Teilweise beobachten diese Unternehmen auch Onion-Services im Tor-Netzwerk auf die Veröffentlichung von abgeflossenen Daten.

[3] https://www.bfdi.bund.de/DE/Service/Anschriften/Laender/Laender-node.html
[4] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.html
[5] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Personen/Vorfall-Experte/Liste-Vorfall-Experte/liste-Vorfall-Experte_node.html
[6] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Listen/Liste-IT-Sicherheitsdienstleister-IS-Revi/liste-it-sicherheitsdienstleister_node.html

Damit diese Unternehmen möglichst effizient arbeiten können sind einige vorbereitende Punkte im Anhang 6.1 dargestellt.

Verbände

Wenn Sie Mitglied in einem Verband sind, können Sie dort ggf. auch von dieser Seite Unterstützung erhalten. Nutzen Sie Ihre Netzwerke und Beziehungen um ggf. Hilfen, Unterstützung, Personalverstärkung, Entlastung, Übernahme von Teilservices als temporäre Alternative, etc. zu erhalten.

Polizeien

Bei einem Angriff auf IT-Systeme werden in der Regel mehrere Straftaten begangen, insbesondere solche nach §§ 202a, 202b, 202c, 303a und 303b StGB. Grundsätzlich wird empfohlen, für alle Cyber-Angriffe bei der Polizei Strafanzeige zu erstatten.

Für betroffene Unternehmen hat das Bundeskriminalamt bzw. haben die zuständigen Landeskriminalämter spezialisierte Anlaufstellen (Zentrale Ansprechstelle Cybercrime, ZACs) eingerichtet, die Opfern von Cyber-Straftaten beratend zur Seite stehen und bei einer Anzeige unterstützen. Eine Liste der Anlaufstellen, sowie eine Broschüre zum Thema finden Sie auf den Webseiten der Allianz für Cybersicherheit[7].

Beachten Sie, dass bei einer Anzeige mögliche Beweise gerichtsfest erhoben und alle Vorgänge entsprechend dokumentiert werden müssen.

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Das BSI ist ein kompetenter Ansprechpartner im Fall eines schweren IT-Sicherheitsvorfalls. Es verfügt über fundierte Kenntnisse bei der Behandlung von Angriffen. Bei folgenden Punkten kann Sie das BSI im Rahmen freier Ressourcen unterstützen:

- Unterstützung durch vorbereitete Dokumente mit Empfehlungen und Vorgehensweisen,
- Vermittlung von (Forensik-)Experten und
- Besprechung von Maßnahmen.

Das BSI kann nur in absoluten Ausnahmefällen im Rahmen seiner gesetzlichen Möglichkeiten selbst aktiv unterstützen. Gehen Sie daher nicht von einer unmittelbaren Unterstützung des BSI bei der Umsetzung notwendiger Maßnahmen aus (Stichwort MIRT)!

Die Vorgabe von § 3 Abs. 1 S. 2 Nr. 18 BSIG lautet: „Unterstützung bei der Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen nach § 5a.“ Ein herausgehobener Fall nach §5a Absatz 2 BSIG liegt „insbesondere dann vor, wenn es sich um einen Angriff von besonderer technischer Qualität handelt oder die zügige Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems von besonderem öffentlichem Interesse ist.“ Insbesondere eine Infektion mit gängiger Ransomware fällt hier regelmäßig nicht darunter. Für Betreiber Kritischer Infrastrukturen bestehen aufgrund entsprechender gesetzlicher Regelungen erweiterte Unterstützungsmöglichkeiten.

Die Zusammenarbeit mit dem BSI erfolgt vertraulich. Das BSI wird keine Informationen zu einem Vorfall an Dritte ohne Ihre explizite Zustimmung weitergeben.

Bei Fragen wenden Sie sich an das BSI-Service-Center[8].

[7] https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/IT-Sicherheitsvorfall/Unternehmen/Kontakt-zur-Polizei/Zentrale-Ansprechstellen-Cybercrime/zentrale-ansprechstellen-cybercrime_node.html

[8] https://www.bsi.bund.de/DE/Service-Navi/Kontakt/kontakt_node.html

3.8 Daten-Leak

Es ist inzwischen üblich, dass die Angreifenden bei einem Ransomware-Angriff auch Daten kopieren und dann mit der Veröffentlichung drohen. Daher sollte die Leak-Seite hierauf beobachtet werden. Sollten Daten des Vorfalls veröffentlicht werden, sollten diese analysiert und Betroffene über den Sachverhalt und entstandene Risiko informiert werden.

3.9 Lösegeld bezahlen?

Im Fall einer bereits erfolgten Verschlüsselung sollten Sie grundsätzlich auf jedwede Form von Erpressung nicht eingehen und kein Lösegeld bezahlen. Stattdessen sollten die Daten nach einer Bereinigung des Netzwerks aus bestehenden und integren Backups zurückgespielt werden. Wurden die Backups jedoch ebenfalls verschlüsselt und wird daher der Versuch erwogen, durch Zahlung des Lösegelds einen Schlüssel zur Entschlüsselung der Daten zu erhalten, denken Sie an folgendes:

- Wenn Sie eine Cyber-Versicherung haben, informieren Sie diese frühzeitig. Häufig gibt Ihnen diese Vorgaben, was Sie tun müssen, damit sie für entstandene Kosten aufkommt.
- Mit einer Lösegeldzahlung finanzieren Sie möglicherweise weitere Angriffe auf Dritte – bitte klären Sie etwaige Zahlungen auf jeden Fall mit den zuständigen Ermittlungsbehörden bzw. mit Ihrer Rechtsabteilung / Rechtsanwälten ab.
- In einigen Fällen konnte die Höhe des Lösegelds in professionellen Verhandlungen durch IT-Sicherheitsdienstleister deutlich reduziert werden.
- Sie haben trotz Zahlung keine Garantie, tatsächlich einen passenden Schlüssel zu erhalten – Sie verhandeln schließlich mit Kriminellen.
- Erhaltene Schlüssel können teilweise für Ihre Daten nicht passend oder die Verschlüsselungsroutine fehlerhaft sein. Fordern Sie daher zu Beginn der Verhandlungen von den Tätern die beispielhafte Entschlüsselung einiger Dateien, um zu verifizieren, dass diese überhaupt im Besitz des korrekten Schlüssels sind.
- Die erfolgreiche Entschlüsselung ersetzt nicht die Neuinstallation der kompromittierten Systeme. Um einen weiteren Zugriff der Täter auf das interne Netzwerk und die erneute Ausbreitung der Schadprogramme auszuschließen, müssen nach der Entschlüsselung zwingend alle Daten gesichert werden und nach einem Neuaufbau des Netzwerks zurückgespielt werden. Dies ist insbesondere wichtig, da die Täter eine Hintertür hinterlassen haben könnten, welche zu einer erneuten Verschlüsselung führen kann – Sie haben ja schon einmal gezahlt, warum also nicht noch einmal.

Sollten Sie entgegen der Empfehlung des BSI trotzdem zahlen, informieren Sie bitte die Polizei. Gegebenenfalls kann diese den Fluss des Geldes verfolgen und die Täter identifizieren.

3.10 Nachbereitung

Denken Sie an eine Nachbesprechung zur Auswertung und Verbesserung.

- Welche langfristigen Maßnahmen müssen ergriffen werden?
- Was ist gut gelaufen, wo gibt es Verbesserungspotenzial?
- An welchen Stellen sollten Sicherheitsmaßnahmen verbessert werden?

Planen Sie eine Revision Ihrer IT durch Externe, sobald die Maßnahmen umgesetzt sind. Die Liste zertifizierter IT-Sicherheitsdienstleister in den Geltungsbereichen IS-Revision und IS-Penetrationstests benennt IT-Sicherheitsunternehmen, die ihre Leistungsfähigkeit in diesen Bereichen bewiesen haben[9]. Darüber hinaus können diese ggf. weitere fallrelevante Angebote machen.

[9] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Listen/Liste-IT-Sicherheitsdienstleister-IS-Revi/liste-it-sicherheitsdienstleister_node.html

Danken Sie Ihren Vertragspartnern und Kunden für das Verständnis, die Geduld und die Unterstützung. Planen Sie mit etwas Abstand ein "Dankeschön" für Ihre an der Vorfallsbewältigung beteiligten Mitarbeiter. Nutzen Sie Ihre Möglichkeiten von Prämien, Sonderurlaub, Abschluss-Party, etc. Auch diese "kleine Investition" rentiert sich langfristig!

4 Incident Response – Technisches Vorgehen

In diesem Kapitel werden technische Maßnahmen vorgestellt, mit denen das Ausmaß des Angriffs eingegrenzt werden kann.

4.1 Ruhig bleiben und geplant handeln

Das Vorgehen bei einem schweren IT-Sicherheitsvorfall ist häufig vom Einzelfall abhängig. Wie lange können die Systeme offline bleiben? Wobei handelt es sich bei diesem Vorfall (Ransomware, Wirtschaftsspionage)? Ist eine Sicherung der Spuren für eine Anzeige gewünscht? Wie ist die Bedrohungslage für Ihre Institution?

Crime-Angriffe werden im Regelfall durch ihre meist aggressive Vorgehensweise nach kurzer Zeit entdeckt, verbreiten sich hierdurch jedoch auch schnell. Eine Infektion mit Ransomware zeigt meist innerhalb von wenigen Tagen bis hin zu zwei Wochen ihre Auswirkung. Die tatsächliche Verschlüsselung von Daten beginnt häufig nachts oder am Wochenende.

Im **Idealfall** sollte der Vorfall zunächst möglichst nicht-invasiv analysiert werden, um einen Überblick zu erhalten und es sollte erst gehandelt werden, wenn der Sachverhalt komplett verstanden wurde.

Nach Möglichkeit sollte der Angriffsweg festgestellt werden, um eine erneute Infektion über diesen Weg zu vermeiden. Schnellschüsse, die leider in der Praxis oft vorkommen, etwa nur ein einzelnes auffällig gewordenes infiziertes System zu bereinigen können dazu führen, dass in kurzer Zeit erneut ein Vorfall eintritt. In manchen Fällen etablieren die Angreifer im Netzwerk Brückenköpfe, welche als Einzige aktiv mit der Außenwelt kommunizieren. Alle anderen kompromittierten Systeme kommunizieren nur mit den Brückenköpfen. Wird jetzt nur der Brückenkopf bereinigt, weil nur dieser in den ersten Analysen aufgefallen ist, kann der Angreifer über zusätzlich angelegte Hintertüren auf den anderen Systemen wieder die Kontrolle über Ihr Netzwerk zurückerlangen.

Dieser Idealfall ist jedoch häufig nicht zu halten. Wenn bereits Systeme verschlüsselt sind oder Hinweise darauf bestehen, dass Systeme mit einer Malware infiziert sind, die häufig **Ransomware** nachlädt (etwa „Trickbot“, das „Ryuk“ nachlädt) sollte rasch gehandelt werden. In diesem Fall sollten die betroffenen Systeme möglichst schnell vom restlichen **Netz getrennt** und nicht mehr mit Verbindung zum Internet betrieben werden. Dazu das Netzwerkkabel ziehen.

Das Ausmaß der erforderlichen Analyse hängt stark vom Einzelfall ab. Wenn alle Systeme verschlüsselt sind ist das ein deutlicher Hinweis, dass das AD kompromittiert ist. In diesem Fall ist es ausreichend, den Einfallsvektor zu finden. Zur Bearbeitung einer Strafanzeige wird es hingegen erforderlich sein, möglichst viele Logs und forensisch gesicherte Systeme liefern zu können.

Wenn die Gefahr einer Infektion weiterer Systeme gebannt ist und Sie nicht zur Fortführung der Unternehmenstätigkeit sofort wieder produktiv gehen müssen, sollte etwas Zeit in die Planung des weiteren Vorgehens der Bereinigung investiert werden.

Das Management sollte frühzeitig informiert und diesem insbesondere die Dimension und die Konsequenzen dieses Angriffs aufgezeigt werden.

4.2 Wo beginnen?

Oberste Regel: Keinesfalls darf eine Anmeldung mit privilegierten Nutzerkonten (Administratorkonto) auf einem potenziell infizierten System erfolgen, während es sich noch im produktiven Netzwerk befindet!

Eine wichtige erste Maßnahme ist die Validierung aller (Admin-)Accounts. Sind alle angelegten Admin-Accounts legitim oder gibt es Accounts, die keinem Mitarbeiter zugeordnet werden können? Gibt es

Accounts von Standardnutzern, die nicht nur über Benutzerrechte, sondern auch über Admin-Rechte verfügen? Diese Accounts könnte die Schadsoftware modifiziert haben und nutzen.

Prüfen Sie, welche Accounts sich auf zentralen Systemen angemeldet haben und zu welchen Zeiten dies geschehen ist. Eine Übersicht über relevante Event-IDs zu Benutzeränderung finden Sie im Anhang 6.5.

Überprüfen Sie auch die Netzwerkmitschnitte auf ungewöhnlichen Netzwerkverkehr. Zusätzlich könnten auch versuchte DNS-Auflösungen auf Clients oder fehlgeschlagene DNS-Auflösungen (NXDOMAIN) am DNS-Server auf eine Schadsoftware hindeuten. Auf betroffenen Systemen kann die lokale Windows Firewall überprüft werden (etwa auf neue RDP-Freigaben).

In den folgenden Kapiteln wird in der Reihenfolge eines Idealfalls aufgezeigt, wie die für eine Analyse des Angriffs benötigten Daten (wie forensische Images, Speicherabbilder und Netzwerkmitschnitte) möglichst fehlerfrei erstellt werden können. Die so gesammelten Daten müssen aber auch ausgewertet werden. Eine sorgfältige Analyse aller dieser Daten und damit die Analyse des Angriffs benötigt in der Regel viel Zeit. Je nach Sorgfaltsbedarf dauern die forensischen Analysen bis zu mehreren Wochen oder gar Monate.

In Kapitel 4.9 werden anschließend einige wichtige Punkte für die Bereinigung dargelegt.

4.3 Forensische Beweissicherung

Jede Aktion, die Sie auf einem kompromittierten System zur Analyse durchführen, kann im schlimmsten Fall dazu führen, dass ermittlungsrelevante Daten unwiderruflich verändert, zerstört oder gelöscht werden. Für eine Beweissicherung sollte daher der erste Schritt sein, ein forensisches Abbild des Systems anzufertigen. Ist das System aktuell eingeschaltet, sollte die einzige Aktion, die noch am Live-System durchgeführt wird, die Erstellung eines forensischen Abbildes des flüchtigen Speichers (Arbeitsspeichers) sein. Danach sollte das System ausgeschaltet werden. Da beim Herunterfahren viele Dateien vom Betriebssystem angefasst und manche Dateien überschrieben werden, sollte ein kompromittiertes System grundsätzlich nicht heruntergefahren, sondern „hart“ der Stromstecker gezogen werden.

Bei der Erstellung eines Festplattenimages ist darauf zu achten, dass ein richtiges forensisches Image, d.h. eine 1:1 Sektorkopie, erstellt wird. Marktübliche Festplatten-Backupprogramme können solche forensischen Images in der Regel nicht erstellen.

Bei virtuellen Systemen reicht es aus, das Verzeichnis der Virtualisierungssoftware zu sichern. Wenn die virtuelle Maschine suspendiert wird, befindet sich im Virtualisierungsverzeichnis zudem ein Dump des Arbeitsspeichers. Dies kann bei der Auswertung der flüchtigen Daten helfen.

Bei physischen Systemen ist dies z. B. mit einer forensischen Live-CD möglich, etwa [10] oder [11]. Die Erstellung eines entsprechenden USB-Sticks zum Booten ist etwa unter [12] beschrieben. Wenn Sie, wie empfohlen, die Polizei oder einen Dienstleister hinzugezogen haben, können diese Sie unterstützen und beraten.

Das infizierte System sollte nicht mehr als notwendig angefasst werden, idealerweise sind die folgenden Arbeiten nur noch an einer Kopie der Daten durchzuführen.

4.4 Umgang mit Logdaten

Bei einem Angriff ist die Auswertung von Logdaten eines der wichtigsten Mittel, um das Ausmaß des Angriffs aufklären zu können. Durch eine Erfassung und die Auswertung von Logdaten der Netzwerk-Kommunikation können Rückschlüsse auf infizierte Systeme getroffen werden und ggf. auch noch unbekannte infizierte Systeme gefunden werden. Jede Institution sollte daher bereits im Vorfeld eine gut geplante Logging-Policy etabliert haben und sicherstellen, dass die Logs auch regelmäßig erzeugt und sicher

[10] https://www.caine-live.net/
[11] https://sumuri.com/product/paladin-edge-64-bit-version-7/
[12] https://www.coalfire.com/The-Coalfire-Blog/August-2017/Forensically-Imaging-a-Microsoft-Surface-Pro-4

gespeichert werden. Sollte so eine Logging-Policy nicht existieren, sollten umgehend die unten genannten Logging-Mechanismen umgesetzt werden.

Neben den technischen sollten auch die rechtlichen Rahmenbedingungen (Datenschutz und Beteiligungspflicht des Betriebs-/Personalrat) für eine solche Speicherung geprüft werden.

Von besonderem Interesse für eine Analyse sind:

- Die Logs des HTTP-Proxy, um HTTP-Datenverkehr zu Command & Control Servern entdecken und nachvollziehen zu können.
- Logs des E-Mail Servers
- Firewall-Logs
- Active-Directory / LDAP-Logs: Gibt es ungewöhnliche Zugriffe (z.B. durch einen Exchange-Admin auf dem AD-Server) oder Zugriffe zu ungewöhnlichen Zeiten?
- File-Access-Logs: Auf welche Dateien konnte zugegriffen werden und welche Daten könnten veröffentlicht werden?

Daneben gibt es noch eine ganze Reihe weiterer Möglichkeiten, insbesondere lokales Loggen auf möglicherweise betroffenen Systemen, wie Sicherheits- oder Systemereignisse bei Windows oder (SSH-)Logins auf Linux Systemen.

Die Auswertung der vielen verschiedenen Logdateien sollte von erfahrenen Netzwerk-Analysten durchgeführt werden, welcher gute Kenntnisse des kompromittierten Netzwerkes hat und entsprechend in der Logdatenanalyse geschult ist.

4.5 Netzwerkverkehr-Analyse

Der Best-Practice und vom BSI empfohlene Ansatz zur Analyse eines laufenden Angriffs ist das Full-Packet-Capturing im Netzwerk. Mit diesem können nicht nur Kommunikations-verbindungen, sondern auch Kommunikationsinhalte aufgezeichnet und analysiert werden. Diese werden benötigt, um zum Beispiel durch einen Angreifer übermittelte Kommandos nachvollziehen zu können oder um festzustellen, welche Informationen zum Angreifer abgeflossen sind. Im Regelbetrieb kann der Einsatz von Full-Packet-Capturing aus Datenschutzsicht problematisch sein. Bei einem konkreten Vorfall sollten aber Netzwerkmitschnitte zur Gefahrenabwehr angefertigt werden. Grundsätzlich sollten vor dem Einsatz des „Full-Packet-Capturing“ der Datenschutzbeauftragte und der Betriebsrat der Institution eingebunden werden.

Bei einem Einsatz von TCPDump bei einem Full-Packet-Capturing muss auf jeden Fall der Parameter „-s0“ gesetzt werden, um die Pakete vollständig aufzuzeichnen.

4.6 Wie loggen?

Die Aufzeichnung der Netzwerkmitschnitte, sowie die Syslogs wichtiger Systeme, sollten auf dedizierten Protokollservern zusammengeführt und archiviert werden. Eine Infektion der verwendeten Loggingsysteme sollte ausgeschlossen werden, ggf. sollten diese neu aufgesetzt werden, falls nicht ausgeschlossen werden kann, dass auch die Loggingsysteme durch den Angreifer kompromittiert wurden. Außerdem kann ein Angreifer alle Logdateien manipulieren, welche lokal auf einem kompromittierten System liegen.

Das Loggingsystem sollte im Optimalfall über eine professionelle Server-Netzwerkkarte verfügen, welche im „Promiscuous“-Mode arbeiten kann. Für die Logdaten müssen je nach Netzwerklast mehrere Terabyte an Speicherkapazität vorgehalten werden.

Es existieren diverse Open-Source-Tools wie TCPDump und Wireshark für die Aufzeichnung und Auswertung der Logdaten. Für die Aufzeichnung sollte man etwa TCPDump verwenden. In den Programmen gibt es immer wieder Sicherheitslücken, die ein Angreifer durch speziell manipulierte Pakete ausnutzen kann. Daher sollten die Logs auch auf einem dedizierten System ausgewertet werden. Daneben

existieren auch kommerzielle Produkte, welche vor allem die Auswertung der Daten durch statistische Analysen oder Visualisierungen vereinfachen.

4.7 Anmerkungen

Folgende Punkte sollten bei einer Auswertung von Logdaten beachtet werden:

- Es sollte ein detaillierter und aktueller Netzplan existieren. Falls kein Plan existiert, sollte dieser sofort erstellt werden. Damit kann geprüft werden, welche Systeme regulär untereinander Daten austauschen und bei welchen eine Kommunikation verdächtig ist.
- Um möglichst schnell mit dem Logging des Netzwerkverkehrs starten zu können, sollten ein dediziertes Logsystem und eine Anleitung zur Nutzung vorbereitet sein. Ansonsten sollte es kurzfristig wie in Kapitel 4.6 beschrieben aufgesetzt werden. Bei einfachen Netzen ohne viel Verkehr kann zunächst auch ein aktuell nicht benötigtes Notebook (frisch installiert) zum Einsatz kommen.
- Bedenken Sie, dass ein kompetenter Angreifer versuchen wird, lokale Logs zu löschen und die Erstellung neuer Logs zu sabotieren.

4.8 Praxishilfe

Im Folgenden finden Sie einige Praxistipps für gebräuchliche Programme, die sich in der Vergangenheit bei der Aufzeichnung und Analyse von Logdaten im Rahmen von Vorfällen bewährt haben.

Squid-Proxy-Log

Beim Einsatz eines Squid-Proxys empfiehlt das BSI, dass neben den reinen Verbindungsinformationen auch Referer, User-Agent und die Anzahl gesendeter Bytes mitgeloggt werden. Eine gute Übersicht, welche Informationen am Proxy geloggt werden sollten, finden sich in dem Artikel „Proxy server logs for incident response“[13].

DNS-Analyse

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 ratsam, DNS-Anfragen am DNS-Server zu loggen oder sogar ein Passive System standardmäßig, auch ohne den Verdacht auf eine Infektion, im Netzwerk im Einsatz zu haben.

Falls keine DNS Logs existieren, sollte die Aufzeichnung aller DNS-Auflösungen am DNS-Server sofort aktiviert werden.

4.9 Bereinigung

Schadprogramme nehmen teilweise tiefgreifende (sicherheitsrelevante) Änderungen am infizierten System vor, die nicht einfach identifiziert und rückgängig gemacht werden können. Das BSI empfiehlt daher grundsätzlich, infizierte lokale Systeme als vollständig kompromittiert zu betrachten und neu aufzusetzen.

Idealerweise sollten alle kompromittierten Systeme zur gleichen Zeit vom Netz genommen werden - zum Beispiel durch gleichzeitige Deaktivierung aller Netzwerkports am Switch. Nach Möglichkeit sollten alle kompromittierten Systeme forensisch gesichert und anschließend komplett neu aufgesetzt werden, um auszuschließen, dass Hintertüren übersehen wurden. Falls bei der Analyse der Infektionsvektor gefunden wurde, sollte dieser geschlossen werden. In jedem Fall sollten die Systeme nach der Neuinstallation komplett aktualisiert und gehärtet werden, bevor sie ans Netz gehen, um eine erneute Infektion auszuschließen.

[13] Proxy server logs for incident response - https://www.vanimpe.eu/2016/10/21/proxy-server-logs-incident-response/

Langfristig sollte das AD neu aufgesetzt und konzipiert werden. Da dies aber ein sehr aufwändiges, zeitintensives Projekt ist, kann eine kurzfristige Maßnahme zur Wiederherstellung der vorübergehenden Arbeitsfähigkeit die Arbeit mit einem überarbeiteten alten AD erfolgen. Kurzfristig besonders wichtig ist es dabei zum Zeitpunkt nach der Bereinigung von sauberen Systemen aus alle Admin-Kennwörter, die Kennwörter aller Dienste / Services / Daemons und alle Kennwörter, die möglicherweise auf infizierten Systemen eingegeben wurden, zu ändern. Ansonsten kann ein Angreifer diese Passwörter weiterhin nutzen und auf die Systeme zugreifen. Überprüfen Sie auch, ob Sie unbekannte Benutzer- oder Administratoraccounts finden.

Die Problematik mit „Golden Tickets“ und Kompromittierungen von Domaincontrollern und Serversystemen (AD und alle domain-joined Systeme neu aufsetzen) ist zu beachten. Sollte es nicht möglich sein alle Systeme direkt in ein neues AD zu migrieren, muss das Passwort des eingebauten Key Distribution Service Accounts (KRBTGT) zweimal zurückgesetzt werden. Dies invalidiert alle Golden Tickets welche mit dem zuvor gestohlenen KRBTGT-Hash und allen anderen Kerberos Tickets erzeugt wurden[14]. In dem Dokument von CERT-EU wird zusätzlich auf die Auswirkungen dieser Maßnahme eingegangen.

Sobald Sie sich hinreichend sicher sind, dass das AD bereinigt wurde könnend Sie sich an die Wiederherstellung der Systeme machen. Hierbei können Systeme für kritische Geschäftsprozesse priorisiert werden. Diese relevanten Geschäftsprozesse können etwa vom Krisenstab in Abstimmung mit der Geschäftsführung identifiziert werden. Damit kann dann ein Kernnetz aufgebaut werden, welches systematisch erweitert werden kann. Wenn Full-Backups vorliegen, können diese auf nackte Systeme eingespielt werden. Wenn nur Backups der Daten vorliegen sollte das System zuvor mit einem sauberen neuen Image initialisiert werden. Löschen Sie dazu die alte Partition und installieren das Betriebssystem erneut.

Arbeiten Sie hierbei wenn möglich mit Kopien der Backups bzw. bei Einsatz von Datenband stellen Sie read-only ein. Damit verhindern Sie, dass , sollten einige Systeme bei der Bereinigung übersehen wurden, auch die Backups im Nachhinein noch infiziert werden.

Nach Möglichkeit sollten Sie für einige Zeit (etwa 2-3 Wochen) jede nicht unbedingt benötigte Remote-Verbindung (RDP, SSH, Terminal-Server, Teamviewer, etc.) blockieren und Verbindungsversuche mitloggen sowie analysieren. Dies könnte einen Hinweis geben, wo noch Schwachstellen existieren könnten. Auch und gerade Administratoren sollten in der Zeit wo immer möglich nur lokal arbeiten können.

Alle auf betroffenen Systemen gespeicherten bzw. nach der Infektion eingegebenen Zugangsdaten sollten als kompromittiert betrachtet und die Passwörter geändert werden. Dies umfasst u. a. Webbrowser, E-Mail-Clients, RDP/VNC-Verbindungen, Benutzer-Logins, Passwörter für Fachverfahren sowie andere Anwendungen wie PuTTY, FileZilla, WinSCP, etc.

Falls Sie schnell mit der Bereinigung begonnen haben und es zu einem erneuten Ausbruch kommt, sollten Sie die Infektionskette genauer untersuchen!

[14] http://cert.europa.eu/static/WhitePapers/UPDATED%20-%20CERT-EU_Security_Whitepaper_2014-007_Kerberos_Golden_Ticket_Protection_v1_4.pdf – insb. Kap. 3.2.

5 Schlussbemerkung und weiteres Vorgehen

Dieses Papier soll Betroffenen helfen, bei der Bewältigung eines schweren IT-Sicherheits-vorfalls keine Fehler in der Anfangsphase zu begehen, die später dazu führen, dass der Angriff nicht bereinigt oder aufgeklärt werden kann. Dieses Papier stellt aber nur den ersten Einstieg in das Incident Handling eines schweren IT-Sicherheitsvorfalls dar, welches sich über Wochen und ggf. sogar Monate erstrecken kann.

Wie in Kapitel 3.1 dargestellt, kann man die Vorfallsbearbeitung in drei Phasen aufteilen. Dieses Papier dient als Unterstützung in den Einstieg von Phase 1 (Analyse). Man sollte sich aber auch frühzeitig Gedanken zum Vorgehen in den nächsten zwei Phasen machen. Parallel zur Analysephase sollte schon der mögliche Übergangsbetrieb (Phase 2) geplant werden. Dort ist ein intensives Monitoring notwendig, da ab diesem Zeitpunkt ein weiterer Datenabfluss verhindert werden sollte. Auch erfordert der sichere Neustart (Phase 3) eine längere Planungsphase, bevor schließlich wieder in einem sauberen Netzwerk gearbeitet werden kann.

Nach Bewältigung des Vorfalls sollten Sie sich Gedanken über die nächsten Maßnahmen machen und diese priorisieren. Ein interner Bericht sollte den Sachverhalt möglichst neutral aufarbeiten. Die bisherigen Schutzmaßnahmen sollten überdacht werden: mögliche Hilfen finden Sie in dem Dokument „Maßnahmenkatalog Ransowmare“[15].

Durch eine bedarfsgerechte Konzeption des Active Directories kann künftig das Risiko eines übergreifenden Vorfalls deutlich gesenkt werden. Durch die Unterteilung in verschiedene Ebenen mit Zugriffseinschränkungen[16] kann eine Ausweitung von Rechten innerhalb eines Netzes erschwert werden. Durch Active Directories mit unterschiedlichen sog. Forests[17] kann eine Ausbreitung von Malware über verschiedene Organisationseinheiten, etwa ein Standort oder Geschäftssegment hinaus, begrenzt werden. Diese Aufgabe erfolgreich umzusetzen ist von enormer Bedeutung, jedoch nicht einfach.

[15] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Massnahmenkatalog.html

[16] https://docs.microsoft.com/de-de/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

[17] https://docs.microsoft.com/de-de/windows-server/identity/ad-ds/plan/forest-design-models

6 Anlagen

6.1 Vorbereitungen für externe Unterstützung

Wie in Kapitel 3.7 beschrieben, ist es für Unternehmen ohne eigenes Forensik-Team in der Regel ratsam, externe Unterstützung für die Analyse des Vorfalls hinzuzuziehen.

Die Erfahrung hat gezeigt, dass folgende Vorbereitungen Ihrerseits es einem externen Unterstützungs-Unternehmen ermöglichen, schnell mit der Bearbeitung des Vorfalls zu beginnen:

Räume:

- Arbeitsraum für 4-8 Mitarbeiter mit freier Wand für Projektor-Anzeige
- Falls möglich ein zweiter Raum (Besprechungsraum) für Meetings, VK/TK

Infrastruktur

- Freier Breitband-Netzzugang (über ein nicht kompromittiertes Netz), für VPN freigeschaltet.
- Arbeitsraum: Nach Möglichkeit mindestens 2x 16A Stromkreisläufe

Daten

- Bereiten Sie Netzpläne vor.
- Klären Sie vorab, welche Logdaten das externe Unternehmen vor Ort analysieren muss und welche es in das eigene Labor mitnehmen darf.

Ansprechpartner:

- Ansprechpartner benennen und die externe Unterstützung ankündigen bzw. die Mitarbeiter persönlich vorstellen
    - Dazu gehören auch Ansprechpartner bei IT-Dienstleistern für relevante Systeme
- Liste der Ansprechpartner erstellen (Name, Telefonnummer, Mailadresse)
  Je nach Umfang / Bedarf in Ihrem Unternehmen die Kontakte zu:
    - Abteilungsleiter IT-Sicherheit für Policy-Kontakte
    - Referatsleiter IT-Sicherheit
    - IT-Sicherheitsbeauftragte
    - Netzwerk-Administrator
    - Firewall-Administrator
    - Pressesprecher / interne Kommunikation

6.2 Kommunikation

Folgende Zielgruppen sollten in der Kommunikation bedacht werden.

Intern

- Presse- / Öffentlichkeitsarbeit
- Vorstand / Aufsichtsrat
- Mitarbeitende
- Call- /Service-Center
- Pforte / Sicherheitsleitstelle
- Juristen
- Datenschutzbeauftragte
- Personalvertretung

Extern

- Polizei (ZAC)
- weitere Behörden (Aufsichtsbehörde, Datenschutzbehörde, BSI)

- Presse und Medien
- Kunden
- Lieferanten
- Regulatoren und Versicherer
- Verbände / Vereinigungen

Mögliche Maßnahmen

- Grundregel: Es kommuniziert nur die Pressestelle (one way) – Kommunikationskanäle zentralisieren
- interne Sprachregelung abstimmen und verteilen
- zeitnah informieren
- Pressemitteilung abstimmen und geeignet veröffentlichen
- Information über Soziale Netzwerke (Bezug auf die offizielle Pressemitteilung)
- Internetpräsenz überarbeiten (Information der breiten Öffentlichkeit)
- Intranet überarbeiten (Information der Mitarbeitenden)
- Informationsfluss aufrechterhalten (Updates!)
- IT-Sicherheitshinweis erstellen
- Medien-Monitoring (Social Media beachten!)

6.3 Punkte einer Pressemitteilung

Die Erfahrung hat gezeigt, dass ein möglichst offener Umgang mit dem Problem auf das meiste Verständnis in der Öffentlichkeit und bei Betroffenen stößt.

Daher sind die wichtigsten Punkte:

- Was ist passiert, was/wer ist betroffen?
- Gibt es Einschränkungen in der (Dienst-) Leistung – insbesondere im Hinblick auf Kritische Infrastrukturen?
- Sind (zum jetzigen Stand) personenbezogene Daten abgeflossen?
- Haben Sie Behörden informiert?
- Haben Sie externe Unterstützung hinzugezogen?
- Botschaft: We care!

Sollten Sie mit der Polizei und/oder anderen Behörden zusammenarbeiten stimmen Sie die Presse- & Medieninformationen intensiv ab um bspw. keine wichtigen Details aus einer Ermittlung zu veröffentlichen.

6.4 Beratungsphasen des Krisenstabes / Projektteams

Folgende Punkte sind für eine Sitzung des Krisenstabes relevant:

- Welche Situation liegt aktuell vor?
  - Vortrag der allgemeinen Informationen
  - Situationsanalyse und Faktensammlung
  - Trennung von Wissen und Vermutung
- Müssen auf Basis der dargestellten Situation Sofortmaßnahmen (ohne weitere Diskussion / Planung) eingeleitet werden?
- Welchen der bestehenden oder absehbaren Probleme kann mit welchen Handlungsoptionen entgegnet werden?
- Welche Risiken, Chancen und Aufwendungen sind mit den verschiedenen Optionen verbunden?
- Kurze Denkpausen für alle – Keine Wortmeldungen – Keine Diskussionen
- Welche der Handlungsoptionen zu den jeweiligen Problemen wird verfolgt?
  - Eine Option je Problem
  - Zweite Option als "Plan B" festhalten

    - Überprüfung der aktuellen Situation bzgl. der Ausführbarkeit der gewählten Option
    - finale Entscheidung der Leitung
- Wer macht was bis wann zur Durchführung der ausgewählten Handlungsoptionen?
- Führen die gewählten Handlungsoptionen zum Ziel?
- Überprüfung der Zielerreichung und ggf. Korrektur der Maßnahmen
- Sonstiges
- Terminierung der nächsten Sitzung

6.5 Event-IDs

Nach folgenden IDs kann in der Windows Ereignisanzeige gefiltert werden, um Änderungen an Benutzeraccounts nachzuverfolgen:

- Event-ID 4720: Erstellung eines Benutzeraccounts
- Event-ID 4722: Aktivierung eines Benutzeraccounts
- Event-ID 4740: Sperrung eines Benutzeraccounts
- Event-ID 4725: Deaktivierung eines Benutzeraccounts
- Event-ID 4726: Löschung eines Benutzeraccounts
- Event-ID 4738: Änderung an einem Benutzeraccount
- Event-ID 4781: Namensänderung

6.6 FAQ

- Kann ich Backups und ggf. infizierte Systeme in einer netzgetrennten VM starten, ohne dass eine Gefahr für Drittsysteme davon ausgeht?
  → Wenn die Virtualisierungssoftware aktuell ist spricht grundsätzlich nichts dagegen. Das BSI hat keine Erkenntnisse, dass im Rahmen der aktuellen Ransomware-Kampagnen Prozessor-Schwachstellen (Spectre, Meltdown, etc.) aktuell ausgenutzt werden.
- Was sind mögliche Einfallspunkte?
  → Client PCs die Mails lesen oder auch Systeme die als Brückenkopf dienen wie Terminal-Server. Aber auch Systeme, die Remotezugänge (RDP, Teamviewer) von außen zulassen.
- Muss ich wirklich alle betroffenen Systeme neu aufsetzen? Reicht es nicht diese mit einem Virenscanner zu bereinigen?
  → Das Problem ist, dass sich Malware tief an verschiedenen Stellen festsetzt, ohne dass dies offensichtlich ist. Oft ist es schneller ein System neu aufzusetzen anstatt viele Stunden zu versuchen es zu bereinigen.
- Wie informiere ich am besten meine Kunden?
  → Wenn Sie direkte, regelmäßige Kontakte haben fassen Sie die Informationen in einer E-Mail zusammen und rufen Sie zusätzlich an. In einer solchen Mail sollten auf keinen Fall Links enthalten sein. Signieren Sie die Mail soweit möglich.
  Sollten keine entsprechende Kontakte haben schreiben Sie die relevanten Informationen auf Ihre Webseite.
  Erstellen Sie zusätzlich einen Frage-Antwort-Katalog. Mögliche Punkte finden Sie unter Punkt 7.3.
- Ich bin von Ransomware betroffen? Heißt das, dass keine Daten abgeflossen sind?
  → Inzwischen ist es üblich, dass Angreifende standardmäßig auch Daten kopieren Hierdurch können etwa Lieferbestätigungen, technische Details von Produkten oder persönliche Daten von internen oder externen Personen veröffentlicht werden.