

Information für Unternehmen

RANSOMWARE

Unternehmen und Institutionen
als Zielscheibe

www.g4c-ev.org



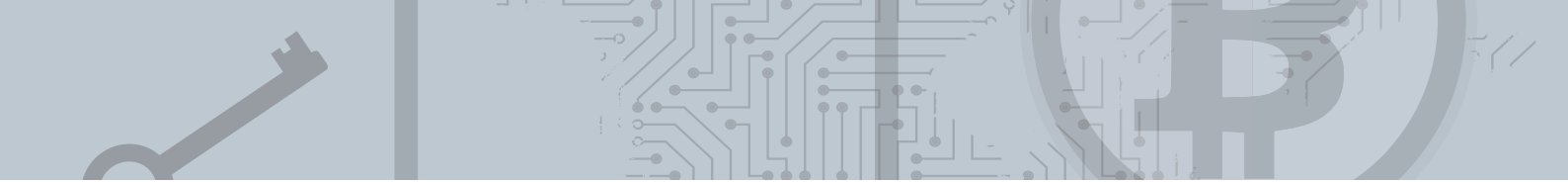
Unsere
Kooperationspartner



Bundeskriminalamt



Bundesamt
für Sicherheit in der
Informationstechnik



Ransomware

Ransomware (engl.): Schadprogramme, mit deren Hilfe Daten auf fremden Rechnern verschlüsselt werden. So soll den eigentlichen Inhabern der Zugriff auf diese Daten unmöglich gemacht werden. Um den für die Entschlüsselung notwendigen Schlüssel zu erhalten, soll das Opfer ein Lösegeld (meistens zahlbar in Bitcoins o. ä.) zahlen.



Wie gelangt Ransomware in die Unternehmen?

Üblicherweise werden solche Schadprogramme großflächig und wahllos per E-Mail versandt. Sofern diese Mails nicht vorab durch zentrale Sicherheitsmaßnahmen wie beispielsweise Spamfilter oder allgemeine Virens Scanner herausgefiltert werden, besteht die Gefahr, dass Empfänger die E-Mails und auch die zugehörigen schadhaften Anhänge öffnen. Verhindern dann nicht weitere Systembeschränkungen oder Arbeitsplatz-Virens Scanner die anschließende Ausführung der Programme, beginnt die automatische Verschlüsselung aller zugänglichen Daten. Ausgereifte Varianten solcher Software versuchen zusätzlich, sich über das interne Netzwerk zu verbreiten. So können sie ein noch weit größeres Erpressungspotenzial erzielen.

Die Folgen können fatal sein

Eine derartige Datenverschlüsselung kann die Verfügbarkeit von Dienstleistungen und Produktionskapazitäten tagelang behindern, im schlimmsten Fall sogar unmöglich machen. Zusätzlich leidet die Reputation des Unternehmens stark durch mediale Negativ-Schlagzeilen: Die Auswirkungen solcher Infektionen lassen sich kaum vor der Öffentlichkeit verbergen¹. Bisher forderten die Erpresser als Lösegeld nur wenige Bitcoins, auf die betroffene Unternehmen meist nicht eingingen. Stattdessen führten sie ihren Betrieb über die Wiederherstellung von Backups fort.

Neue Gefahren durch gezielte Angriffe

Ein neuer Trend besteht darin, das Erpressungspotenzial gezielt bis auf die nachhaltige Vernichtung nahezu aller Datenbestände eines Unternehmens oder einer Institution inklusive Backups auszudehnen.

Gelingt den Tätern eine solche Vollverschlüsselung, können sie deutlich höhere Lösegeldsummen fordern: Hier würde die Einschränkung von Dienstleistungen oder Produktionskapazitäten nicht nur kurze Zeit andauern, sondern es droht im schlimmsten Fall sogar der dauerhafte Verlust aller vorhandenen Daten.

Dies kommt für viele Firmen faktisch einer drohenden Einstellung des Geschäftsbetriebes gleich.

Information und Hilfe

Diese Broschüre soll Unternehmen und Institutionen dabei unterstützen, das Phänomen Ransomware und die davon ausgehende Bedrohung zu verstehen. Sie soll dabei helfen, präventive und detektive Gegenmaßnahmen zu konzipieren und für den Ernstfall Hilfsmittel an die Hand geben.

¹ Öffentlich bekannt gewordene Beispiele waren z.B. das Lukaskrankenhaus Neuss (10.02.2016), die Deutsche Bahn (13.05.2017) oder der dänische Logistikkonzern Maersk (26.01.2018).

Wie gehen die Täter vor?

Üblicherweise erfolgen die Angriffe via E-Mail mit entsprechenden schadhafte Anhängen. Deren Ausprägungen können variieren. In der Praxis sind es jedoch sehr häufig Office-Dokumente (z. B. Word-Dateien), die nach dem Öffnen Schadsoftwarekomponenten nachladen. Derartige E-Mails können potenziell jeden Mitarbeiter eines Unternehmens erreichen. Die vielzitierte Warnung, niemals Anhänge von E-Mails unbekannter Absender zu öffnen, ist nicht praktikabel, wenn die Dateien sich als Initiativbewerbungen in der Personalabteilung ausgeben, bei Kunden-Hotlines oder bei Vertriebsmitarbeitern mit Außenkontakt ankommen. Zusätzlich gilt: Aktuelle Tätergruppen verwenden auch Mailverkehr, den sie bei früheren Angriffen auf andere Unternehmen erlangt haben, und nehmen darauf Bezug. So sind sie in der Lage, scheinbar bekannte Absender vorzutäuschen. Erfolgt dieses Vorgehen massenhaft und gezielt, wird es auch als „Dynamit-Phishing“ bezeichnet.

Oft läuft die technische Infektion dann in mehreren Schritten ab. Zunächst erfolgt die Installation eines „Downloaders“, der weitere Schadsoftware wie die eigentliche Ransomware, aber auch Fernwartungssoftware („Remote Access Tools“) zur weiteren Erkundung der IT-Infrastruktur des Unternehmens nachlädt².

Varianten der Vollverschlüsselung einschließlich Backups

■ Verbreitung im gesamten Netzwerk

Die initiale Ransomware versucht – u.a. über Netzlaufwerke – administrative Accounts wie Domain-Admins und Backup-Accounts zu übernehmen. Ein gängiges Vorgehen ist das Erraten von Passwörtern oder massenhaftes Ausprobieren („Brute-Force“). Aufgrund oftmals ver-

wendeter Standardpasswörter und mit Hilfe ausgeklügelter Passwortlisten sind die Angreifer damit erfolgreicher, als gemeinhin angenommen. Dabei nutzen sie ebenso nicht gepatchte Schwachstellen aus, beispielsweise im Intranet. Gelingt eine dieser Methoden, meldet sich die Schadsoftware aktiv bei den Tätern, dass hier (abweichend vom Normalfall) ein möglicherweise deutlich lukrativeres Opfer zu erwarten ist. Die Täter versuchen dann im Nachgang oft noch manuell, etwa via Remote Access Tools, größere Kontrolle über die IT-Infrastruktur des Unternehmens zu erlangen und insbesondere alle Backup-Möglichkeiten völlig unbrauchbar zu machen.

■ Vorab geplante und gezielte Angriffe

Angreifer verschaffen sich vorab weitreichende Informationen über die jeweiligen Unternehmen oder Institutionen. Das geschieht über sogenanntes Social Engineering, um das Umfeld via soziale Netzwerke, Telefonanrufe unter Vortäuschung falscher Identitäten und Phishing-Mails zu erkunden. Dies dient auch dazu festzustellen, ob eine lukrative Ausgangslage vorliegt. Außerdem können nachfolgende Infektionen mit Ransomware so gezielt platziert werden. Im Zuge solcher Sondierungen können sich Tätergruppen auch weiter im Netzwerk bewegen und zusätzliche Informationen über das Unternehmen sammeln. Aus diesen Erkenntnissen leiten einige Täter sogar die Höhe von Lösegeldern ab und stellen dann Forderungen, die sich das Unternehmen ihrer Meinung nach leisten kann, ohne völlig in seiner wirtschaftlichen Existenz gefährdet zu sein.

² Zum Nachschlagen in einer Web-Suche: Historisch prominente Bezeichnungen von Ransomware aus 2016/2017 lauteten z.B. „Locky“ oder „WannaCry“, die per 2018/19 relevanten Schadsoftwarefamilien tragen Bezeichnungen wie „Emotet/Trickbot“, „Ryuk“ „GandCrab“.

Aus der Praxis

Es ist typisch, dass Täter mit den Bemühungen um eine Vollverschlüsselung der anvisierten IT-Infrastruktur am Freitagabend beginnen, weil dies ungestörtes Arbeiten aufgrund der Abwesenheit der Mitarbeiter am Wochenende verspricht. Die IT-Störungen zeigen sich dann meist erst am Montagmorgen, wenn Computer nicht starten, Telefonanlagen, Mail-Server, Web-Präsenzen und das Electronic-Banking-System ausfallen oder Backups verschlüsselt sind. Üblich ist auch, dass in der Folge ein englischsprachiges Schreiben auftaucht, in dem eine größere Lösegeldsumme gefordert wird – zahlbar in einer Kryptowährung und bei gezielten Angriffen durchaus ein fünf- bis siebenstelliger Euro-Betrag.

Welche Maßnahmen schützen effektiv vor Infektionen mit Ransomware?

■ Grundabsicherung gegen eingehende Schadsoftware

Die Basiskomponente für die Abwehr eingehender Schadsoftware sind Maßnahmen wie technische Spam- und Malware-Filter beim zentralen E-Mail-Eingang, gegebenenfalls auch am Web-Proxy und an anderen externen Schnittstellen, sowie auch auf dem Desktop des Endnutzers, auf Servern, File Shares etc. Insbesondere das Bundesamt für Sicherheit in der Informationstechnik (BSI) hält hierfür passende und Hinweise und Hilfestellungen bereit³.

■ Bewusstsein bei Mitarbeitern und Geschäftspartnern schaffen

Zunächst sollten vor allem Mitarbeiter über die Bedrohung aufgeklärt werden. Das Bewusstsein bei Geschäftspartnern und Lieferanten zu steigern, ist eine weitere wichtige und unverzichtbare Basismaßnahme. Wie diese Punkte

zu handhaben sind, hat die Heise Mediengruppe sehr anschaulich in einem Bericht über den Umgang mit einem Trojaner-Befall im eigenen Hause aufbereitet⁴.

■ Einen Schritt weiter denken

Es ist immer damit zu rechnen, dass per Mail eingehende Malware die erste Hürde der zentralen Abwehr unentdeckt passiert. Daher sind zusätzlich auch klare interne Richtlinien zum Umgang mit verdächtigen E-Mails, beziehungsweise Mails mit verdächtigen Anhängen, notwendig. Da auch Mitarbeiter ohne tiefere IT-Kenntnisse Ziel solcher Mails sein können, müssen entsprechende Handlungsempfehlungen einfach auffindbar, verständlich formuliert und vor allem unterstützend sein. Neben dem Hinweis, Absenderadressen Buchstabe für Buchstabe zu prüfen, sollte jeder Mitarbeiter Hilfe an die Hand bekommen, falls er vor dem Dilemma steht, eine verdächtige Mail zu öffnen und so eine Infektion auszulösen oder sie zu löschen und damit eine möglicherweise wichtige Mail zu vernichten.

Bewähren kann sich hierfür die Einrichtung einer internen Mailbox, an die unternehmensinterne Empfänger verdächtig erscheinende Mails samt Anhängen vor dem Öffnen zur Prüfung schicken können. Idealerweise sollten dort dann sogenannte Sandbox-Lösungen⁵ und/oder Security-Experten eine eingehendere Prüfung vornehmen und das Ergebnis zeitnah an den Mitarbeiter zurückmelden. In einigen wenigen Unternehmen ist dies bereits gelebte Praxis, in (zu) vielen anderen Unternehmen und Institutionen aber nicht. Mitunter besteht diese Möglichkeit zwar, wird den Mitarbeitern aber noch nicht ausreichend kommuniziert.

³ „BSI warnt vor gezielten Ransomware-Angriffen auf Unternehmen“ (https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/BSI_warnt_vor_Ransomware-Angriffen-240419.html) und „Maßnahmen zum Schutz vor Emotet und gefährlichen E-Mails im Allgemeinen“ (<https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/E-Mailsicherheit/emotet.html>).

⁴ „Trojaner-Befall: Emotet bei Heise“ (<https://www.heise.de/ct/artikel/Trojaner-Befall-Emotet-bei-Heise-4437807.html>).

⁵ Eine Sandbox bezeichnet eine von der firmeneigenen IT-Infrastruktur isolierte Umgebung, die eine reale IT-Umgebung simuliert. Dort können verdächtige Dateien ausgeführt und deren Auswirkung auf Computersysteme geprüft werden.

Welche Maßnahmen können einer gezielten Datenvernichtung vorbeugen?

■ Überprüfung der Backup und Recovery-Maßnahmen

Ein Backup-Konzept, das primär für den Ausfall von Speichermedien konzipiert wurde und dazu dient, in diesem Fall die Geschäfte normal weiterführen zu können, kann unter Umständen völlig untauglich gegen Angriffe mit Verschlüsselungstrojanern sein. Um Unternehmen und Institutionen davor zu schützen, sind Offline-Backups bzw. Speichermedien notwendig, die nicht jederzeit per Netzwerk oder File Shares erreicht und überschrieben werden können. Zu einem guten Backup-Konzept gehört außerdem auch immer auch das regelmäßige praxisnahe Testen der Recovery-Fähigkeiten. Hierbei wird geprüft, ob aus den erstellten Backups ein fehlerfreies Produktivsystem wiederhergestellt werden kann.

■ Sparsame Verwendung privilegierter und administrativer Zugänge

Je mehr und je öfter Benutzerkonten mit erweiterten Zugriffsrechten für die tägliche Arbeit Verwendung finden, desto höher ist das Risiko einer versehentlichen Infektion. Entsprechende Konten, wie das des Domänenadministrators, sollten also nur für die Aufgaben verwendet werden, für die sie tatsächlich vorgesehen sind. Ein Login über das Netzwerk für lokale Administratoren und auch lokale Administrator-Accounts sollten – wann immer möglich – über Gruppenrichtlinien deaktiviert werden. Sollten entsprechende Accounts doch benötigt werden, empfiehlt sich ein spezifisches lokales Administrator-Passwort. Dafür bietet beispielsweise Microsoft das kostenlose Tool „Local Administrator Password Solution“ (LAPS) an, das Passwörter automatisch verwaltet und in

einem gesonderten Verzeichnis speichert.

■ Passwörter für administrative Accounts sehr sorgfältig erstellen

Die Wahl sicherer, nicht zu erratender Passwörter ist für solche Accounts von besonderer Bedeutung. Default- oder auch Standardpasswörter bieten definitiv keinen ausreichenden Schutz. Aber auch eine davon abweichende Passwortwahl will wohlüberlegt sein. Sichere Passwörter sollte eine Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthalten, die so nicht in Wörterbüchern vorkommen und sollten sich auch nicht auf persönliche Informationen beziehen.

■ Security Patches auch im Intranet

Das praxisrelevante Grundproblem von Infektionen mit Ransomware besteht meist darin, dass Mails mit schadhaften Anhängen die erste Hürde des Virenschutzes am zentralen Mail-Server unentdeckt überwunden haben. Wird die Schadsoftware durch Öffnen des Anhangs dann aktiviert, befindet sie sich bereits im internen Netz. Daher empfiehlt es sich, auch im vermeintlich gegen Angriffe von außen geschützten Intranet Security Patches so zeitnah wie möglich zu installieren. Sind – etwa bei älteren Industrieanlagen, Produktionsstraßen oder medizinischen Geräten – die Installationen von Security Patches nicht oder nur stark verzögert möglich, sollten diese Maschinen vom Rest des Netzwerks so weit wie möglich isoliert werden.

■ Überprüfung von Verbindungen zu Dienstleistern und Geschäftspartnern, insbesondere bei ausgelagerten IT- und Cloud-Lösungen

Da sich fortgeschrittene Ransomware über alle vorgefundenen Netzverbindungen auszubreiten versucht, kann dies potenziell auch Netzverbin-

dungen zu Dienstleistern und Geschäftspartnern betreffen. Um möglichst sicherzustellen, dass über diese Verbindungen keine Infektionen verbreitet werden, sollten die entsprechenden Zugriffsmöglichkeiten und Berechtigungen für das Netzwerk überprüft werden. Dies sollte auch für den umgekehrten Weg beachtet werden, um die Cybersicherheit der Geschäftspartner sicherzustellen.

Aufbau eines Systems zur Notfallplanung und Krisenvorsorge

■ Notfallplanung und Prüfung der bestehenden Maßnahmen

Viele Unternehmen haben bereits Vorkehrungen für schwerwiegende Sicherheitsvorfälle und Krisenszenarien getroffen und Notfallpläne erstellt. Decken diese aber auch die Szenarien der potenziellen Vollverschlüsselung der gesamten IT- und Datenbestände ab? Eine eingehende Prüfung und gegebenenfalls Ergänzung der Notfallplanung ist in jedem Fall ratsam. Eine externe Überprüfung durch ein anerkanntes und qualifiziertes IT-Security-Unternehmen kann hier eine gute Investition in die Zukunft darstellen und bietet einen wertvollen Direktkontakt für den späteren Ernstfall. Zertifizierte IT-Sicherheitsdienstleister, die gewisse geprüfte Qualitätsstandards erfüllen, listet das BSI auf seiner Website auf⁶.

■ Kommunikationsfähigkeit für den Notfall sicherstellen

Im Ernstfall kann die gesamte IT-Infrastruktur eines Unternehmens verschlüsselt und damit funktionsunfähig sein. Dies betrifft dann auch E-Mail-Programme, Telefax- und Telefonanlagen, einschließlich aller Kontaktdaten. Doch genau in dieser Situation ist es notwendig, intern mit den Mitarbeitern und der Presseabteilung



und extern mit Strafverfolgungsbehörden, IT-Security-Firmen, Geschäftspartnern, Medien, Anwälten, Banken etc. kommunizieren zu können. Eventuell stehen Diensthandys als funktionsfähiges Kommunikationsmittel zur Verfügung, auch diese jedoch vielleicht nur mit eingeschränktem Zugang zu internen Informationen. Daher sollten Notfalldokumente wie beispielsweise Kontaktlisten zu den wichtigsten internen und externen Gesprächspartnern immer auch als Papiausdruck oder zumindest separat auf USB-Stick oder CD vorliegen. So können Unternehmen auch unabhängig von potenziell kompromittierten oder ausgefallenen Systemen darauf zugreifen.

■ Zahlungsfähigkeit sicherstellen

Auch wenn Unternehmen für einen längeren Zeitraum informationstechnisch lahmgelegt sind, müssen sie ihren Zahlungsverpflichtungen nachkommen. Dies kann bei kompromittierten Systemen eventuell nicht mehr möglich sein. Im Zuge des Aufbaus eines Sicherungssystems sollte daher auch Kontakt zur Hausbank aufgenommen werden. Diese kann u.U. einen

⁶ „Zertifizierte IT-Sicherheitsdienstleister“ (https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Stellen/Stellen_node.html).

Online-Zugang zu den Unternehmenskonten für den Notfall vorbereiten, der auch außerhalb der technischen Infrastruktur des Unternehmens funktioniert.

■ **Vorbereitende Kontaktaufnahme und Vernetzung**

Hilfreich für die Abwehr von Cybercrime-Angriffen sind Kontakte zu Branchenverbänden und zu anderen Unternehmen der Branche oder Lieferkette, aber auch zu Institutionen wie G4C und vor allem zu den Strafverfolgungsbehörden. Diese haben für derartige Themen und Fälle „Zentrale Ansprechstellen Cybercrime der Polizeien für Wirtschaftsunternehmen“ (ZAC⁷) eingerichtet. Es kann auch sinnvoll sein, sich vorab mit seiner Hausbank zu dieser Thematik in Verbindung zu setzen. Viele Banken kennen das Thema aus dem Tagesgeschäft mit Firmenkunden gut und haben somit teilweise vielfältige Maßnahmen im Portfolio. Diese reichen von präventiver Bewusstseinsaufklärung über Ersatzoptionen für den Zahlungsverkehr bis - für den äußersten Notfall - hin zu reaktiver Unterstützung bei Kontakten zu Strafverfolgungsbehörden oder auch bei der Bitcoin-Beschaffung.

■ **Cybersecurity- oder Vertrauensschaden-Versicherungen**

Grundsätzlich besteht die Möglichkeit, sich gegen etwaige Schäden aus Cyberangriffen zu versichern. Welche Risiken und Schäden eine solche Versicherung wirklich abdeckt, muss individuell geprüft werden. In der Regel spielt es für Versicherungen eine wichtige Rolle, dass geeignete, präventive Maßnahmen bestehen. Ob und inwieweit es hier sinnvoll sein kann, sogar Totalverluste oder etwaige Lösegeldzahlungen abzusichern, muss jedes einzelne Unternehmen für sich selbst prüfen und dann mit der jeweiligen Versicherung besprechen.

Wie können Unternehmen für eine Früherkennung sorgen?

■ **Auf dem Laufenden bleiben**

Aus der vorbereitenden Kontaktaufnahme und Vernetzung können Unternehmen frühzeitig erfahren, wie sich aktuelle Angriffsszenarien entwickeln. Darüber hinaus stellt insbesondere der Twitter-Account des CERT-Bund (BSI)⁸ eine sehr gute und aktuelle Informationsquelle dar.

■ **„Information Sharing“-Initiativen beitreten**

Durch Information Sharing können beteiligte Unternehmen Angriffsmerkmale erfahren, die sie in ihre eigenen Schutzmechanismen einspielen können. Solche sogenannte Indicators of Compromise (IOCs), sind beispielsweise typische Merkmale von eingehenden schadhaften E-Mails und ihren Anhängen oder Servernamen und IP-Adressen, zu denen sich aktive Malware zu Steuerungszwecken verbindet.

■ **Eigenständig Zusatzinformationen erheben und teilen**

Unter anderem über die präventive Nutzung einer zentralen Ansprechstelle im Unternehmen für verdächtige Mails kann das Unternehmen mehr über die eigene reale Bedrohungslage erfahren und gewisse Erkenntnisse dann gegebenenfalls auch mit anderen Unternehmen teilen. Freiwilliges Information Sharing zwischen Unternehmen ist ein gegenseitiges Geschäft zum Nutzen aller Beteiligten.

⁷ https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html

⁸ <https://twitter.com/certbund>

Wie ist zu handeln, wenn der Ernstfall eintritt?

■ Zeit ist jetzt Geld!

Kompetenzen und erwartete Handlungsweisen sollten jedem Beteiligten im Unternehmen möglichst klar sein. Kommunikationschaos ist nicht nur unprofessionell, sondern kostet wertvolle Zeit und hat gegebenenfalls auch nachhaltige Konsequenzen auf das Betriebsklima im Unternehmen und zum Management.

■ Auf präventiv geknüpft Kontakte zurückgreifen

Im Zuge des Aufbaus eines Notfall und Krisenvorsorge-Systems sollten bereits Kontakte zu den ZAC und zertifizierten Sicherheitsdienstleistern hergestellt worden sein. Auf diese gilt es nun so schnell wie möglich zuzugehen, um Unterstützung zu suchen.

■ Hände weg von der Technik und externe Expertise einholen

Dieser durchaus pragmatische, erste Hinweis kann sinnvoller sein als halbherzige Rücksicherungsversuche. Diese können noch mehr Schaden anrichten und eine Entschlüsselung selbst nach Bezahlung und Erhalt der Schlüssel unmöglich machen. Es ist besser, frühzeitig die jeweilige ZAC der Polizei einzuschalten und sich an eigens befähigte IT-Forensik-Unternehmen zu richten. Sollten Sie nicht schon vorher im Rahmen der Notfallplanung gute und vertrauenswürdige Kontakte zu entsprechenden Dienstleistern geknüpft haben, dann untenstehend eine Quelle zu entsprechenden durch das BSI qualifizierten und geprüften „Notfall-IT-Sicherheitsdienstleistern“⁹.

Wird eine Infektion mit Ransomware erkannt, ist **schnelles Handeln gefragt**. Hierfür spielt die umfassende Vorbereitung aller Beteiligten eine wichtige Rolle.

Denn nur wenn **Abläufe und Verantwortlichkeiten** feststehen und bekannt sind, können Unternehmen langfristige finanzielle und kommunikative Risiken minimieren.

Ein allererster und wichtiger Rat dazu lautet: Haben Sie nicht selber ausgeprägtes Knowhow in solchen Themen der Cybercrime-Bekämpfung, holen Sie sich zeitnah externe Expertise dazu (s.u.)

■ Im Zweifel: Erstmal Abschalten!

Hat ein Unternehmen den Angriff schon frühzeitig entdeckt und verfügt über eigene oder zeitnah organisierte externe, qualifizierte IT-Security-Expertise, können die gegnerischen Aktivitäten beobachtet werden. Dabei sollten ihre Auswirkungen jedoch kontrolliert und eingegrenzt werden. Ist dies nicht möglich, sollte eine vollständige Netzabtrennung, beziehungsweise eine Abschaltung möglichst aller Komponenten in Betrachtung gezogen werden, bis Klarheit darüber herrscht, welche Systeme betroffen sind und welche nicht.

■ Auf Nummer sicher gehen

Die nachgeladenen Schadprogramme werden häufig in der ersten Zeit nach ihrer Verbreitung nicht von Standard-Antivirus-Software erkannt. Solche Malware nimmt aber teilweise tiefgreifende Änderungen an infizierten Systemen vor,

⁹ Qualifizierte Dienstleister bei Cyberangriffen (https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Dienstleistungen/Qualifizierte_Dienstleister/QDL_node.html), hier insbesondere der Abschnitt zu „APT-Response“, d.h. für die Reaktion nach einem gezielten Angriff.

die nicht einfach rückgängig gemacht werden können. Die grundsätzliche Empfehlung ist daher, derlei infizierte Systeme als vollständig kompromittiert zu betrachten. Auch auf solch betroffenen Systemen gespeicherte, beziehungsweise nach einer Infektion eingegebene Zugangsdaten sollten als kompromittiert behandelt und die Passwörter geändert werden.

■ **Fokus auf administrative Accounts, Netzwerk-Segmentierung und Security Patches**

Haben die Täter es geschafft, sich Zugang zu administrativen Accounts zu verschaffen, ist eine Wiedereinspielung ohne Änderung der zugehörigen Accounts und Passwörter in der Regel erfolglos. Auch ein Wiedereinspielen eines veralteten Security Patch-Levels aus dem Backup mag ebenso wirkungslos verpuffen.

■ **Meldefristen beachten**

Unternehmen sollten auch etwaige Meldefristen beachten. In der Regel gilt: Wo Schadsoftware eingebracht werden konnte, sind vermutlich auch Daten abhandengekommen. Bei personenbezogenen Daten drohen Unternehmen bei nicht eingehaltenen Meldefristen beispielsweise aufgrund der DSGVO unter Umständen harte Strafen.

Thema Lösegeld: Wie sollten Unternehmen sich verhalten?

BSI, Strafverfolgungsbehörden, Sicherheitsexperten und auch G4C raten dringend davon ab, Lösegelder zu zahlen. Dadurch sollen kriminelle Geschäftsmodelle nicht weiter gefördert werden, zumal es gegebenenfalls Alternativen gibt, um die infizierten Unternehmensdaten zu entschlüsseln. Im Fall einer Lösegeldzahlung ist zudem nicht garantiert, dass Unternehmen oder Institutionen die notwendigen Schlüssel erhalten oder dass diese wirklich funktionieren. Gelingt es aus eigener Kraft, die Geschäftsfähigkeit wiederherzustellen, sollten Unternehmen also keinesfalls auf Forderungen der Erpresser eingehen.

Solche allgemeinen Empfehlungen helfen allerdings kaum, wenn ein Unternehmen aufgrund einer Vollverschlüsselung samt Backups oder einer nicht funktionierenden Recovery handlungsunfähig gemacht ist. Steht ein Unternehmen oder Institution dann vor der Wahl, den Geschäftsbetrieb einzustellen oder Lösegeld zu zahlen, kann im Einzelfall eine Zahlung in Betracht gezogen werden. Bevor eine Entscheidung hierzu gefällt wird, sollten Betroffene aber unbedingt externe Expertise hinzuziehen:



- Gegebenenfalls gibt es tatsächlich Möglichkeiten, etwaige Entschlüsselungs-Codes anderweitig zu beschaffen oder die Daten zu rekonstruieren. Bei der im Markt befindlichen fortgeschrittenen Ransomware ist dies zwar mittlerweile relativ unwahrscheinlich, eine Ersteinschätzung von Experten – sofern die Schadsoftwarefamilie identifiziert werden konnte – geht aber meist schnell und lohnt einen Versuch.
- Es ist keineswegs einfach, unvorbereitet und in kurzer Zeit hohe Eurobeträge in Kryptowährungen zu beschaffen. Nicht selten werden Unternehmen aber täterseitig unter Zeitdruck mit Androhung von sich erhöhenden Lösegeldforderungen konfrontiert¹⁰. Hier benötigen Betroffene zeitnah Experten, die sie in dieser Situation unterstützen. Einen Aufschub der Zahlung wird ein Unternehmen meist ohnehin erfragen müssen. Auch hierbei ist professionelle Unterstützung angeraten.
- Fortgeschrittene Ransomware-Täter, die Unternehmen gezielt angreifen, haben normalerweise ein „Reputationsinteresse“ daran, dass auch ihre Entschlüsselungsverfahren funktionieren. Chancen auf eine Wiederherstellung über diesen Weg als allerletzter Rettungsanker sind also unter Umständen durchaus vorhanden. Wie hoch diese Chancen tatsächlich sind, können aber nur mit der Materie und Lage vertraute Experten einschätzen.

Betroffene Unternehmen sollten eine solche absolute Notfalloption der Lösegeldzahlung niemals als Ausrede für den Verzicht auf präventive Handlungen nehmen. Die Chance auf eine Rettung durch die Zahlung der geforderten Summe dürfte auch im positivsten Licht kaum besser als 80 zu 20 stehen.



Stattdessen sollten sich Unternehmen der Tatsache bewusst sein, dass eine „post mortem“-Wiederherstellung des Systems, sei es aus den Recovery-Daten oder aus dem Entschlüsselungscode nach der Lösegeldzahlung, auch erst die Hälfte des Wege ist. Die Täter kennen sich nun in den jeweiligen Unternehmen und in ihrer IT-Infrastruktur recht genau aus: Um erneute Angriffe oder Infektionen zu vermeiden, müssen Geschädigte auch die übrige Hälfte des Weges einer mehr oder weniger vollständigen Neuaufsetzung ihrer IT-Landschaft gehen.

Umso zentraler sind daher die Absicherung der unternehmenseigenen IT-Strukturen, ein umfassendes internes und externes Informationsmanagement sowie ein wertvolles Netzwerk aus relevanten Behörden und branchengleichen Firmen. Denn auch beim Thema Ransomware gilt: Vorsorge ist besser als Nachsorge.

¹⁰ Exemplarischer Auszug aus den Botschaften einer der Ransomware-Tätergruppierungen: „Countdown to double price: 2 days“, mit zusätzlich entsprechend rückwärts laufender Uhr.



Als gemeinnütziger Verein hat sich das German Competence Centre against Cybercrime (G4C) zum Ziel gesetzt, präventiv, ermittelnd und reaktiv gegen Angriffe im Cyberraum vorzugehen. G4C fungiert so als Know-how-Träger, Frühwarnsystem und Initiator eines regelmäßigen Austauschs über Bedrohungen aus dem Netz. Operative Kooperationspartner sind das Bundeskriminalamt (BKA) und das Bundesamt für Sicherheit in der Informationstechnik (BSI). Darüber hinaus besteht auch international ein Informationsaustausch mit relevanten Stellen zur Bekämpfung von Cyberangriffen.

Die Arbeit des Vereins basiert auf vier Säulen: G4C baut sukzessive eine aktuelle Datenplattform neben dem direkten persönlichen Austausch als Frühwarnsystem aus, übernimmt Datenausleitungen für das BKA und andere Ermittlungsbehörden, und engagiert sich in der Aus- und Fortbildung sowie bei Zuverlässigkeitsüberprüfungen zur Kompetenzstärkung von Cybersicherheitsbeauftragten.

Gründer und Initialmitglieder von G4C sind Banken und Versicherungen; der Verein weitet seine Kompetenz jedoch konsequent auf weitere Branchen aus.

Alle Inhalte dieser Broschüre, insbesondere Texte, Bilder und Grafiken, sind urheberrechtlich geschützt. Die Verbreitung und Verwertung ist gestattet, solange diese nicht-kommerziell erfolgt. Die Vervielfältigung und Bearbeitung außerhalb der Grenzen des Urheberrechts bedürfen der schriftlichen Zustimmung von G4C. Die Verwendung von Auszügen aus der Broschüre ist nur mit Quellenangabe gestattet.

KONTAKT

Eintrag im Vereinsregister
Wiesbaden VR 6806

www.g4c-ev.org

Stand: November 2019

German Competence Centre
against Cybercrime e. V. (G4C e. V.)

Borsigstraße 34
65205 Wiesbaden

Telefon: +49 6122 178 4800

Fax: +49 6122 178 4803

E-Mail: info@g4c-ev.org