Verschlüsselungstrojaner

Kopfschmerz IT-Security

Informationssicherheit ist ein schwieriges Fach: Viele unscharf klingende Begriffe und abstrakte Konzepte machen das Thema schwer zugänglich. Am Ende hat man viel Aufwand und Geld investiert – und trotzdem hat es einen eiskalt erwischt.

MARCUS HEINZE UND WERNER SPIEGL

Verschlüsselungstrojaner haben 2016 die IT und ihre betreibenden Organisationen großflächig bedroht. Diese Art des Angriffs enthält neben vielen älteren und bekannten Methoden auch neue Verfahren, auf die die meisten technischen Infrastrukturen nicht ausreichend vorbereitet waren. Im Februar meldete heise.de: »Ransomware-Virus legt Krankenhaus lahm«, und beschrieb, wie ein deutsches Klinikum ernsthaft in seiner Arbeit behindert wurde, weil der Trojaner wesentliche Teile der Infrastruktur beeinträchtigte.

Es gibt Berichte, in denen Stadtverwaltungen und andere Einrichtungen sich gezwungen sahen, geforderte Lösegelder zu zahlen: Die Betroffenen erhielten daraufhin den Schlüssel und eine Anleitung, wie die Dateien wieder herzustellen seien. Ein ausgeklügeltes Geschäftsmodell mit 100-prozentiger »Kundenorientierung« ist hier nicht nur zu vermuten.

Es ist für Viren- und Malware-Scanner schwierig, einen bestimmten Cryptotrojanertypen zu erkennen. Hinzu kommt eine durchdachte und effektive IT-Infrastruktur im Hintergrund. In der Regel erfolgt die eigentliche Infektion durch eine sehr schlanke Angriffssoftware. Diese lädt die Module für die Verschlüsselung nach und meldet den Schlüssel und ein paar Informationen zurück. Die Malware verändert sich auf diese Weise kontinuierlich und die Schutzsoftware ist beständig dabei, diesen Veränderungen hinterherzulaufen: Der Vorteil liegt hier eindeutig bei den Angreifern. Dafür benötigen die Angreifer eine performante und effektive Serverinfrastruktur, da die Infektionsrate gerade in der Zeit unmittelbar nach der Freisetzung des Trojaners sehr hoch ist.

Wenn technische Einrichtungen wie Firewalls und Malware-Schutz nicht funktionieren beziehungsweise nicht ausreichen, was dann? Kampflos dem Angreifer ergeben? Wenn man sich die Auswirkungen einmal vor Augen führt, ist dies keine sinnvolle Option. Tatsächlich darf man sich von den Versprechen der Tool- und Gerätehersteller nicht täuschen lassen. Dennoch verrichten deren Lösungen ihre Aufgaben zuverlässig und sind durchaus sinnvoll. Warum passieren dennoch solche Infektionen?

Wie so oft lautet die Antwort: Es gibt keine einfache »One-Size-Fits-All«-Lösung, mit der sich das Problem aus der Welt schaffen lässt. Die Aufgaben und das Umfeld jeder einzelnen Firma, jeder Kommune und eines jeden Krankenhauses sind unterschiedlich. In der Folge sind auch die notwendigen Maßnahmen nicht überall die gleichen.

Sicherheit beginnt damit, dass man sein Geschäft und seine Infrastruktur kennt. Schon bei der Kenntnis letzterer hapert es häufig. Techniker sind meist sehr gut darin, pragmatische Lösungen aufzubauen, die sich als ausgesprochen langlebig erweisen. Nach dem Motto: Nichts hält so lange wie ein gutes Provisorium. Solche Konstrukte sind aber in den seltensten Fällen dokumentiert – es handelt sich schließlich um eine Übergangslösung.

Geschäft und Infrastruktur sind zudem einem ständigen Wandel unterworfen. Die heutige Zeit fordert eine schnelle und (geschäftlich) intelligente Reaktion der Firmen auf alle Eventualitäten. Reagieren sie nicht, werden sie vom Markt überrollt und das Geschäft bricht ein. Eine einmalige Bestandsaufnahme der IT-Sicherheit reicht nicht aus – diese

Dinge müssen stets aktuell gehalten werden und man muss sich immer wieder damit auseinandersetzen.
Im Alltag ist das ein Problem: In der Regel werden für diese Themen keine Kapazitäten freigehalten, da dies aus wirtschaftlicher Sicht nicht zu rechtfertigen ist. Liegt der Anspruch also gerade mal in der Gewährleistung des Betriebes und Geschäftes, bleibt für Themen wie Sicherheit wenig Zeit. Übrig bleibt die Hoffnung, dass einfache Lösungen wie eine neue Firewall oder ein wirksamerer Malware-Schutz ausreichen. Die Cryptotrojaner beweisen, dass dies leider nicht der Fall ist.
Diese Tatsache verursacht bei den IT-Verantwortlichen Kopfschmerzen. Eine schnelle Lösung wie ein Aspirin hilft hier nicht, aber es gibt einen Weg, der – sowohl was Ziel als auch Aufwand angeht – überschaubar ist und gleichzeitig das Kerngeschäft im Fokus hat.

Angriff und Verteidigung in der Praxis

Schaut man sich Unternehmen an, die sich erfolgreich gegen solche Angriffe zur Wehr setzen, erkennt man, dass etwas Vorbereitung und gesunder Menschenverstand fast schon ausreichen. An ein paar Beispielen aus der täglichen Praxis lässt sich dies veranschaulichen.

Fallbeispiel 1

Der Teamleiter eines mittelständischen IT-Dienstleisters war auf der Suche nach neuem Personal. Das Unternehmen leistete bereits eine ganze Menge für IT-Sicherheit: Es gab sowohl Verhaltensrichtlinien als auch technische Schutzeinrichtungen; die Mitarbeiter waren geschult und sensibilisiert für das Thema. Der Teamleiter nutzte das Internet also mit der gebotenen Vorsicht. Der Informations-Link, den er anklickte, stammte aus einer vertrauenswürdigen Quelle. Dass sich hinter dem Link ein Office-Dokument (in diesem Fall: Microsoft Word) verbarg, war nicht zu erkennen. Der Cryptotrojaner, den er somit aktivierte, war neu und dem Virenscanner unbekannt: Er schlug ohne Gegenwehr zu. Alarmiert holte der Teamleiter den IT-Service des Unternehmens zu Hilfe. Dieser reagiert gekonnt: Der infizierte Rechner wurde umgehend vom Netz getrennt (Sofortmaßnahme Nr. 1).
Dennoch war in der Folge ein zentraler Bestandteil der Infrastruktur beeinträchtigt – der Fileserver. Diesen nutzten die Teamleiter für ihre tägliche Dokumenten-Arbeit. Der File-Server wurde daraufhin offline genommen (Sofortmaßnahme Nr. 2), die betroffenen Bereiche gelöscht (Sofortmaßnahme Nr. 3) und die entsprechenden Dateien aus der letzten Sicherung wieder hergestellt (Sofortmaßnahme Nr. 4). Mit geringen Datenverlusten war die Infrastruktur nach zwei Stunden wieder »sauber«.
Die Auswirkungen hielten sich in Grenzen, weil grundlegende, vorbereitende Maßnahmen (preventive actions) ergriffen wurden, um überhaupt Sofortmaßnahme Nr. 4 zu ermöglichen:

- Es gab ein geprüftes, zuverlässiges Backup. Dieses braucht man nicht nur für böswillige Angriffe, sondern auch, um gegen technische Ausfälle und Bedienfehler wie versehentliches Löschen abgesichert zu sein.
- Der Service hatte ein erprobtes Verfahren, um mit dem Ereignis umzugehen.
- Für das betroffene System existierte ein Wiederherstellungs- und Wiederanlaufplan. So konnten alle Maßnahmen gezielt durchgeführt werden und der Zeit- und Datenverlust hielt sich in Grenzen.
- Die Reichweite des genutzten Accounts war begrenzt. Der Anwender hatte nur im notwendigen Umfang Zugriff auf Dateien und Daten. Dies begrenzte den Schaden und damit auch die Menge an Daten, die wiederhergestellt werden musste.
- Die Analyse des Firewall-Logs ermöglichte eine Auskunft über die Herkunft des Trojaners. Die Quelle konnte informiert werden.

Die ergriffenen Maßnahmen sind weitgehend »nicht-technischer« Natur. Es handelt sich um einfache, organisatorische Maßnahmen, mit denen der Schaden minimiert werden konnte.

Fallbeispiel 2

Das zweite Beispiel verhält sich in gewisser Weise ähnlich. Bei dem Betroffenen handelte es sich um eine Praxisklinik, welche hauptsächlich orthopädische Verletzungen betreut und kleinere chirurgische Eingriffe durchführt. Der Angriff wurde erst bemerkt, als eine Verwaltungskraft feststellte, dass weite Teile der Infrastruktur nur noch aus MP3-Dateien bestanden.
Die IT-Infrastruktur der Praxisklinik wurde durch einen externen Dienstleister betreut. Dieser fuhr zunächst die Infrastruktur herunter. Die zentralen Dienste wurden aus dem Backup wieder hergestellt. Parallel dazu durchforstete man die Clients nach der Ursache für das Problem. Auch hier war es ein Cryptotrojaner, der sich auf einem Rechner im Behandlungsraum eingeschlichen hatte. Die entsprechende Maschine wurde ausgetauscht und neu aufgesetzt.
Bis die zentralen Dienste wiederhergestellt waren und die Clients als gesäubert erachtet werden konnten, war die Praxisklinik nicht in der Lage, Patienten zu betreuen. Bei der Patientenmenge, die eine solche Einrichtung üblicherweise zu bedienen hat, ist dies nicht akzeptabel. Entsprechend hoch war das Stressniveau.
Abgesehen von dem Schadensaspekt direkt in der Infrastruktur, bereitete die Frage nach einem möglichen Datenabfluss Sorge. Mit einer geeigneten Protokollierung der Netzübergangspunkte ließ sich dieses Problem allerdings schnell verneinen. Auch die Wiederherstellung der Dienste verlief reibungslos und der Schaden konnte begrenzt werden. Unter dem Strich war dieser Vorfall allerdings wesentlich schädlicher als im ersten Fall. Was waren die Ursachen?

- Die Rechner in den Behandlungsräumen erlaubten weitgehenden Zugriff auf die Infrastruktur.
- Die Benutzer waren sich der Gefahren nicht ausreichend bewusst und nutzten die gefährdete Infrastruktur für Internet-Zugriffe.

Grundlegende Maßnahmen halfen aber auch hier weiter und erlaubten es, den Schaden zu begrenzen:

- Ein erprobtes Backup erlaubte eine Wiederherstellung der Systeme.
- Der Schutz wichtiger Infrastruktur (hier das Praxisverwaltungssystem) verhinderte einen kritischen Datenverlust. Die Zugriffe beruhten auf anderen Mechanismen, die der Trojaner nicht nutzen konnte.
- Das Logging am Netzübergang konnte beweisen, dass kein Datenabfluss stattgefunden hatte.
- Die Daten lagen alle auf dem Fileserver. Dieser wurde regelmäßig gesichert. Eine Datenwiederherstellung war somit möglich. Der betroffene Client konnte daher einfach aus der Infrastruktur entfernt und nach einer Neuinstallation wieder in Betrieb genommen werden.

Eines wird an diesem Beispiel deutlich: Je weniger umfassend die Schutz-Maßnahmen sind, desto gravierender wirkt sich ein solches Ereignis aus. Dennoch sind die zu unternehmenden Maßnahmen nicht komplexer Hightech-Natur. Es handelt sich um einfache, durch gesunden Menschenverstand gebotene Verfahren.

Fallbeispiel 3

Ein drittes und letztes Beispiel verdeutlicht das mögliche Schadenspotenzial. In diesem Fall handelte es sich bei dem Betroffenen um ein medizinisches Versorgungszentrum mit mehr als zehn Standorten in der Umgebung, über 200 Mitarbeitern und 250 PC-Arbeitsplätzen. Jeder einzelne Standort, also jede Arztpraxis, kommuniziert dabei mit einem zentralen IT-Standort.
Dieser zentrale IT-Standort stellt eine mögliche Brücke für Schadsoftware dar. Datenbestände wiederum sind nur über Zugriffsprotokolle erreichbar: Der einzelne Client hat daher nur Zugriff auf die direkt angeschlossene Peripherie und erreicht keine anderen Systeme. Ähnlich wie im vorausgehenden Fallbeispiel traf es auch hier ein Clientsystem. Durch die großflächige Verschlüsselung von Dateien war der Client nicht mehr nutzbar. Eine sofortige Überprüfung der gesamten Infrastruktur ergab, dass alle anderen Teile der Infrastruktur nicht beeinträchtigt wurden. Der restliche Standort konnte normal weiterarbeiten. Entsprechend einfach waren die notwendigen Abhilfemaßnahmen. Der betroffene Client wurde durch einen frisch aufgesetzten ersetzt und das Problem war ausgestanden.
Die Beschränkung des Zugriffs hat größeren Schaden verhindert. Auch dabei handelt es sich in erster Linie um eine organisatorische Maßnahme. Durch entsprechende Technik wird sie realisiert. Der Geschäftsführer erläuterte, ein operativer Ausfall koste das Zentrum einen fünfstelligen Betrag pro Tag. Hinzu käme der Vertrauensverlust bei den Patienten, wenn das EDV-System nicht funktioniert und beispielsweise

auf handschriftliche Dokumentation zurückgegriffen werden müsste.

Der Ansatz: Informationssicherheits-Managementsystem

Jedes Geschäft, jede Infrastruktur ist anders. Wie trifft man also die richtigen Maßnahmen? IT-Security-Experten setzen auf ein Informationssicherheits-Managementsystem, kurz ISMS. Es handelt sich hierbei nicht etwa um ein technisches System, sondern um die organisatorische Integration der Informationssicherheit in das Unternehmen. Das Vorgehen ist dabei immer das Gleiche:

- Zunächst sollte definiert werden, welche Systeme, Netze und Informationsspeicher für den Geschäftsbetrieb wichtig sind.
- Im zweiten Schritt gilt es zu bestimmen, wie Systeme, Netze und Informationen aufgebaut sind.
- Dann sollte man sich fragen, was diesen Systemen passieren kann.
- Zu guter Letzt sollte eruiert werden, welche Schritte nötig sind, um den Schaden zu begrenzen.

Aus diesen Punkten leiten sich letztlich die Maßnahmen ab, die getroffen werden müssen, um ein angemessenes Sicherheitsniveau zu erreichen. Wie das ISMS schließlich genau gestaltet ist, hängt von der jeweiligen Unternehmensstruktur ab. Am Ende stehen die technischen Maßnahmen. Diese setzen dann gezielt an und können so ihre volle Leistungsfähigkeit entfalten.

ISMS – genauso wie Qualitätsmanagementsysteme – wurden von Expertengremien genormt. Die ISO 27000 und die dazugehörigen Normen, die weitere Details beschreiben, liefern eine Blaupause, um ein solches ISMS in aller Tiefe aufzubauen.

Die hier dokumentierten Anforderungen sind allerdings nicht von allen IT-Organisationen leistbar. Gerade kleine Unternehmen, aber auch der Mittelstand tun sich schwer, der geforderten Tiefe standzuhalten. Der zusätzlich entstehende Aufwand für Dokumentation, die Ermittlung von Bedrohung und Gefährdung sowie das Ableiten von Risiken und deren Behandlung sind nicht überall leistbar. – Also doch wieder nur Standardmaßnahmen treffen und hoffen?

Unterhalb der ISO-Norm haben sich diverse andere Organisationen bemüht, vereinfachte Blaupausen zu schaffen. Eine besonders einfache kommt aus dem Versicherungsumfeld: die Richtlinie VdS 3473 – Cyber-Security für kleine und mittlere Unternehmen (KMU).

Aufgrund der potenziellen Schadenshöhe sehen sich viele Unternehmen gezwungen, Versicherungen gegen solche IT-Risiken abzuschließen. Ähnlich wie beim Brandschutz fordern die Versicherer eine gewisse Vorsorge ein, um das Restrisiko zu versichern. Allerdings wissen die Versicherer auch um die begrenzten Möglichkeiten vieler Unternehmen und haben daher ein einfach umzusetzendes und mit geringen Mitteln zu betreibendes ISMS erarbeitet. In der VdS-Richtlinie 3473 ist dies niedergelegt. Der VdS auditiert Unternehmen auch auf Wunsch. Mit einem solchen Zertifikat kann man den Versicherungen gegenüber nachweisen, dass man mit dem Thema IT-Sicherheit im Grunde professionell umgeht. Das verbleibende Restrisiko kann man dann zu günstigeren Prämien versichern.

Die Macher der Richtlinie hatten die Kapazitäten der kleinen IT-Organisationen im Blick. Die Elemente der ISO 2700x sind hier im Grunde alle bereits angelegt. Man ging nach dem Pareto-Prinzip vor: Mit 20 Prozent Aufwand lassen sich demnach 80 Prozent des Ergebnisses erzielen. Und 80 Prozent sind allemal besser, als sich blind allen IT-Gefahren auszusetzen.

Das ISMS kann im Laufe der Zeit hin zu einer ISO 2700x weiterentwickelt werden. Die Macher haben auf Kompatibilität geachtet. Wenn also ein Unternehmen am Ende tatsächlich auch ein Zertifikat nach ISO 27001 braucht, dann ist die Anstrengung, die bereits in die Umsetzung der Richtlinie geflossen ist, nicht verloren, sondern stellt eine stabile Basis dar. Cryptotrojaner sind mit einem solchen ISMS nicht mehr bedrohlich und auch die Kopfschmerzen verschwinden. (ne)

MARCUS HEINZE

CIO, Senior-IT-Consultant
Astrum IT GmbH

WERNER SPIEGL

Senior Managing Consultant
Astrum IT GmbH