Strategie gegen Ransomware

Gerüstet für Erpresser

Viele Unternehmen fühlen sich gut gewappnet für Ransomware-Angriffe. Aber sie sollten das gut hinterfragen und sich nicht auf dem Status quo ausruhen, denn die Folgen solcher Angriffe können gravierend sein. Angreifer und Verteidiger befinden sich im ständigen Katz-und-Maus-Spiel. Zu einer umfassenden Strategie zur Abwehr von Ransomware und ähnlichen Angriffen gehören neben der Prävention die Vorfallbehandlung und Notfallpläne.

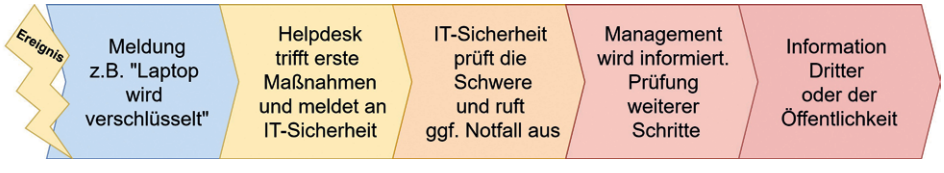
Ein kurzer Faktencheck: Ransomware ist Schadsoftware, die meist per E-Mail verbreitet wird. Sie versteckt sich in Anhängen und Links, die zu speziell erstellten Websites führen. Einmal aktiviert, sperrt sie den Zugriff auf Geräte oder verschlüsselt die darauf befindlichen Daten. Die Angreifer fordern für die Freigabe Lösegeld (englisch „ransom"), das meist in Bitcoins zu zahlen ist. Oft aber sind die Daten, die in die Hände der Kriminellen fallen, unwiederbringlich verloren.

Einfach den PC verschlüsseln war gestern – moderne Ransomware versucht, Schaden auf verschiedenen Ebenen zu verursachen. Emotet zum Beispiel lauert im Hintergrund, sucht sich selbst Verbreitungswege und kann sogar die Verbreiter kontaktieren. Das Programm verschlüsselt erst, wenn sicher ist, dass das Opfer den größtmöglichen Schaden erleidet. Die Wiederherstellung aus einem Backup kann helfen, aber die Datenmengen sind so groß, dass Unternehmen sie häufig nur online sichern. Offline-Medien, zum Beispiel Bänder, sind kaum noch im Einsatz und ihre Funktion auch oft nicht überprüft. Hacker kennen das und versuchen, Backups unbrauchbar zu machen: Bleibt ein Angriff über Tage und Wochen unbemerkt, ist das Backup eventuell längst befallen. Entweder lassen sich die Daten gar nicht oder nur mit großem Aufwand und unvollständig zurückspielen. Bei einer einfachen Wiederherstellung besteht zudem das Risiko, dass die Zerstörung wieder von vorne anfängt. Cybervorfälle erfordern deshalb ein strategisches Vorgehen: Prävention, Behandlung von Vorfällen, Wiederherstellung des Normalbetriebs, Analyse des Vorfalls, Anpassung und Weiterentwicklung der Sicherheitskonzepte und Prozesse.

Zur Prävention ist die gesamte IT-Architektur so aufzubauen, dass eine Infektion sich nicht ungehindert ausbreiten kann. Netzwerksegmentierung ist hier unumgänglich. Per Segmentierung kann die IT den Datenfluss zwischen den Netzwerkbereichen gezielt kontrollieren. Ein ausgefeiltes Monitoring ist ein weiterer wichtiger Baustein zur Früherkennung von Angriffen. Virenscanner reichen nicht aus, da Schadsoftware die Erkennung unterwandern kann. Auch auf die Meldungen betroffener Mitarbeiter zu warten ist keine Option: Bis diese eintreffen, kann das System schon infiziert sein. Das Monitoring sollte alle Systeme und Dienste überwachen, die für geschäftskritische Prozesse relevant sind. Es sollte die Abhängigkeiten zwischen Sensoren zur Event-Auslösung wo immer möglich aggregieren, denn das verbessert die Meldungen. Man sollte sicherstellen, dass alle Systeme im Normalbetrieb auf „grün" stehen, also ohne Warnung. Sonst verlässt sich niemand mehr auf diese Anzeige. Dann sollte man jede Unregelmäßigkeit beachten: Kontaktaufnahme mit bekannten C&C-Servern (Command and Control, die „Steuersysteme" der Angreifer), auffällige Zugriffe auf Storage-Systeme oder Active Directory etc.

Das IT-Team sollte das Monitoring aktuell und vollständig halten und regelmäßig hinterfragen, ob die beobachteten und überwachten Systeme und Sensoren ausreichen. Server, Clients, Netzwerkkomponenten, Virenschutz, Anwendungen – gibt es vielleicht neue Systeme und Angriffsvektoren? Wenn möglich, sollten zentrale Monitoring- und Alarmierungslösungen zum Einsatz kommen. Niemand kann permanent auf die verschiedenen Logs der Firewall, Server und Virenschutzsysteme starren und dabei die Übersicht bewahren. Auch eine Alarmierungs- oder Meldungsflut aus verschiedenen Systemen während eines Vorfalls ist nicht zielführend. Die Zahl der Tools zur Überwachung und Alarmierung ist so gering wie möglich zu halten, um effizient zu sein. Denn jede überflüssige oder sich unnötig wiederholende Meldung birgt die Gefahr der Desensibilisierung.

Unternehmen sollten den Notfall üben, ihre Mitarbeiter auf Cyberangriffe vorbereiten und sie für IT-Sicherheitsthemen mit Security-Awareness-Programmen sensibilisieren. Die Maßnahmen können vielfältig sein, darunter Scheinangriffe mit Phishing-Mails oder Red-Team/Blue-Team-Wettkämpfe, bei denen Mitarbeiter in die Rolle von Hackern schlüpfen. Das ist unterhaltsam und hat das Ziel, Wissen zu vermitteln und die Aufmerksamkeit für Bedrohungen zu erhöhen. Auf Seiten der IT-Techniker geben regelmäßige Funktionstests des



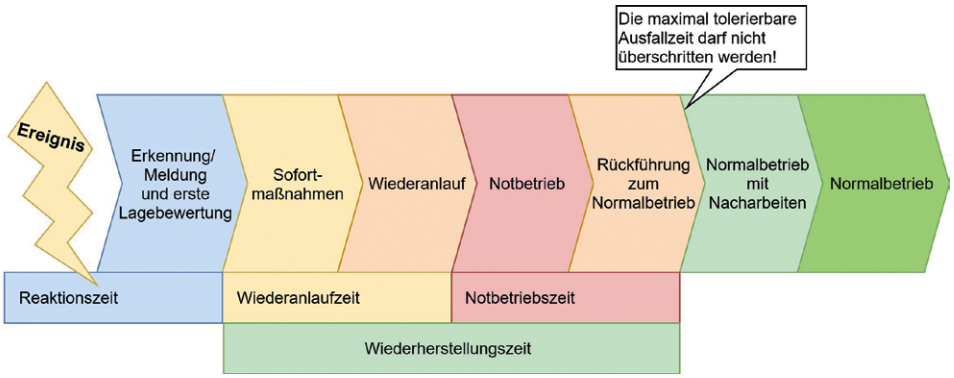
Vereinfachtes Beispiel für einen Meldeweg. Bild: VZM

Backups einen Einblick, ob die Daten vollständig und intakt sind. Disaster-Recovery-Tests auf anderer Hardware geben Auskunft, ob eine Wiederherstellung nach Totalausfall überhaupt funktioniert. Denn eine Systemsicherung, die man nicht zurückspielen kann, ist nichts wert. Die Administratoren benötigen Routine, und die Erfahrungswerte zum Aufwand einer Wiederherstellung sind hilfreich für den Wiederanlauf.

Die Leitplanken bei einem Vorfall sind klare Verantwortlichkeiten, bekannte Meldewege und kontrollierte, geübte erste Reaktionen (Notfallpläne) und eine geordnete Kommunikation. Was am Anfang schiefläuft, kostet nachher viel Zeit und Mühe. Die Maßnahmen: Legen Sie eine Meldestelle für Cybervorfälle fest. Meist ist dies der Helpdesk. Geben Sie den Mitarbeitern die Möglichkeit, Vorfälle schnell zu melden. Vermitteln Sie ihnen das Bewusstsein, dass auch scheinbar einfache Vorfälle meldewürdig sind. Befähigen Sie die Meldungsempfänger, die Lage zu bewerten und erste Hilfe zu leisten. Dazu sind Schulungen hilfreich, aber auch die Entwicklung einer Bewertungsmatrix, die verschiedene Szenarien umreißt und erste Notfallmaßnahmen beschreibt.

Entwickeln Sie Notfallpläne. Diese benennen die Verantwortlichen und beschreiben Vorgehensweisen, etwa die Abschaltung und Abschottung von Netzsegmenten. Notfallpläne sind ein sehr effizientes Werkzeug. Die Beteiligten setzen sich während der Entwicklung mit den Schadensszenarien auseinander und bekommen einen Blick auf das, was kommen könnte. Notfallpläne geben Sicherheit, da sie die grundlegenden Handlungsanweisungen vorgeben. Im Idealfall ermöglichen sie es, fehlende Personalressourcen auszugleichen, sofern die Prozesse detailliert beschrieben und die Zugangsrechte geklärt sind.

Bestimmen Sie ein Notfallteam. Das Team sollte aus erfahrenen Mitarbeitern aus der IT, dem Informationssicherheitsbeauftragten, dem Datenschutzbeauftragten und den betroffenen Bereichen bestehen. Legen Sie fest, wer die Kommunikation nach außen übernimmt. Identifizieren Sie Trigger, ab



Notfallablauf in Anlehnung an den BSI-Standard. Bild: VZM

denen man externe Expertise hinzuzieht. Idealerweise ist das Team für den Tätigkeitszeitraum vom Tagesgeschäft befreit und verfügt über ausreichend Mandat, um die Maßnahmen wirkungsvoll und zeitnah umsetzen zu können. Auch Zugangsrechte sind im Notfall ein wichtiges Thema: Was ist, wenn verantwortliche Administratoren nicht erreichbar sind? Halten Sie Notfallkonten und Bedienhilfen für alle wichtigen Systeme vor – aber bitte sicher und nicht einfach an der Rezeption in einem Notizbüchlein.

Eine vorher abgestimmte Informations- und Kommunikationsstrategie unterstützt dabei, die richtigen Stakeholder und gegebenenfalls die Öffentlichkeit zum richtigen Zeitpunkt zu informieren. Wurden personenbezogene Daten durch den Angriff offengelegt, vernichtet, verändert oder verloren und führt dies zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen, besteht eine Melde- und Informationspflicht an die Datenschutz-Aufsichtsbehörde des jeweiligen Bundeslandes (gem. Art. 33 DSGVO). Die 72-Stunden-Frist beginnt erst zu laufen, wenn der Verantwortliche weiß, dass eine Meldepflicht besteht. Man muss und darf sich einige Stunden Zeit nehmen, um den Sachverhalt gründlich zu untersuchen. Für Auftragsverarbeiter besteht eine unverzügliche Meldepflicht lediglich an den Verantwortlichen. Eine Information der Betroffenen hängt von den konkreten Umständen der jeweiligen Situation ab, also wenn die Schutzverletzung ein „gesteigertes Risiko“ für deren Rechte und Freiheiten erzeugt. Klare Informationen und die glaubwürdige Darstellung, dass man die Situation kompetent behandelt, schützt vor Imageschäden nach innen und außen. Eine Liste der Ansprechpartner zu den verschiedenen Themen (intern wie extern) sollte jederzeit greifbar und bekannt sein.

Normalbetrieb wiederherstellen

Die Wiederherstellung von Systemen muss den Anforderungen des Betriebs entsprechen: Jedes Unternehmen hat für Betriebsprozesse unterschiedlich tolerierbare Ausfallzeiten, festgelegt durch die Fachbereiche oder das Management. Bei einem Totalausfall gilt es, die Systeme innerhalb dieser Zeiten wieder anzufahren, inklusive der Neubeschaffung von Hardware. Der Richtwert ist, sofern vorhanden, das Business-Continuity-Management. Es gilt, die Wiederherstellung basierend auf den Datenbeständen zu priorisieren und zu planen. Sollte die Wiederherstellungszeit länger dauern als die tolerierbare Ausfallzeit, müssen Maßnahmen geplant sein. Sind Kapazitäten zu erweiten? Ist es möglich, auf temporäre Ressourcen (RZ und Mitarbeiter) zurückzugreifen? Auch muss der Notbetrieb festgelegt sein, also der Betrieb mit einem Minimum an Diensten und Daten für einen beschränkten Zeitraum.

Hacker sind nicht dumm, sie gehen mit der Zeit, finden neue Wege und Sicherheitslücken. Verteidiger müssen ständig nach Veränderungen und Auffälligkeiten Ausschau halten. Ein effizientes, kontinuierlich weiterentwickeltes Konzept für den Umgang mit Cyberangriffen ist dabei essenziell.

André Lauterbach/wg

André Lauterbach ist IT-Sicherheitsberater bei VZM (Von Zur Mühlen'sche), www.vzm.de.