Toolkit für Notfallmaßnahmen:

WIE MAN AUF EINEN RANSOMWARE-ANGRIFF REAGIERT- 12 SCHRITTE

Alle unternehmen sollten davon ausgehen, dass sie früher oder später mit einem ransomware-angriff konfrontiert werden. Die wichtigste frage ist, wann. Vorbereitung ist der schlüssel. Dies ist ein leitfaden über dringende massnahmen, die zu ergreifen sind, wenn ihr unternehmen von einer katastrophe betroffen ist.

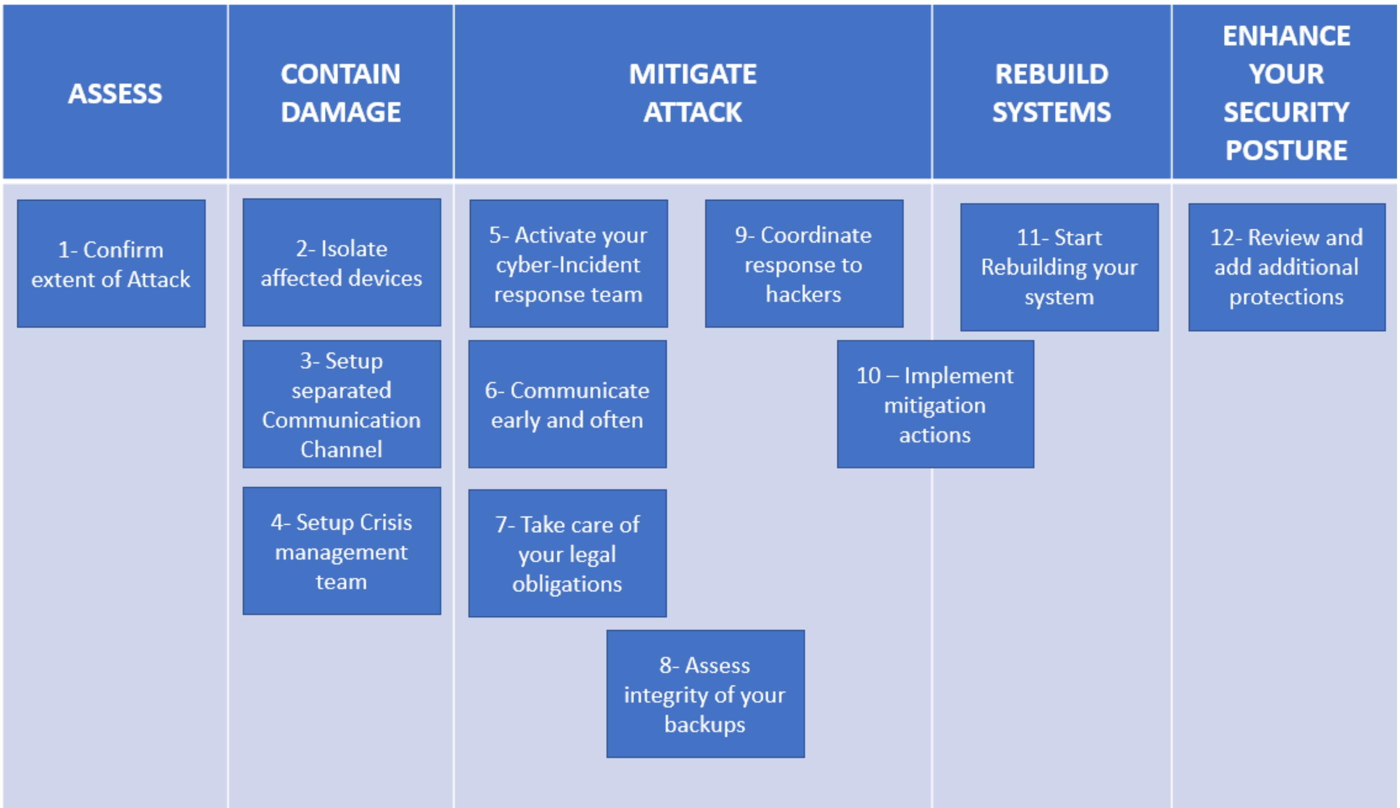
Vorbereitung ist das A und O bei einem Ransomware-Angriff. Das Hauptziel besteht darin, sicherzustellen, dass Unternehmen vorbereitet sind und nicht improvisieren müssen, sobald eine Katastrophe eintritt, was zu zusätzlichen Fehlern führt, die einen noch größeren Datenverlust zur Folge haben können.

Zur Vorbereitung gehört auch, dass Sie sich vergewissern, welche Teams Sie brauchen (Technik, Krise, Kommunikation, ...) und wie diese Personen effizient erreicht werden können. Während der Vorbereitung (d.h. Ihr Playbook ist verfügbar, Sie haben es mit einer Übung getestet), stellen Sie sicher, dass dies auch einen Prozess umfasst, um alles auf dem neuesten Stand zu halten.

Die im Folgenden beschriebenen Schritte sind die Mindestmaßnahmen, die Sie im Falle eines Ransomware-Angriffs ergreifen müssen, hoffentlich durch Anwendung Ihrer Notfallpläne.

Die Wiederherstellung nach einem Ransomware-Angriff ist nicht in wenigen Stunden erledigt, sondern dauert in der Regel Wochen oder Monate. Entscheidend ist jedoch, dass in den Stunden nach einem bestätigten Angriff Maßnahmen ergriffen werden.

Visuelle Schritte auf hohem Niveau



1. Bestimmen und bestätigen Sie das Ausmaß des Ransomware-Angriffs

Der Wiederaufbau von Systemen ist NICHT der erste Schritt in Ihrem Reaktionsplan.

Beurteilen Sie das Ausmaß des Ransomware-Angriffs, indem Sie sich darauf konzentrieren, was verschlüsselt und/oder potenziell exfiltriert wurde. Eine Antwort auf diese Frage ist entscheidend für die Aktivierung eines Reaktionsplans.

Dieser Reaktionsplan wird auch nützliche Erkenntnisse über interne und externe Fragen liefern, die Ihre Führung, Ihre Mitarbeiter und Ihre Kunden haben könnten.

Es ist schwierig, einen Reaktionsplan zu erstellen, wenn Sie das Ausmaß des Angriffs nicht kennen. Versuchen Sie zu dokumentieren, welche Daten sich auf den verschlüsselten Rechnern befanden, und suchen Sie nach Daten, die exfiltriert worden sein könnten.

2. Betroffene Geräte isolieren

Isolieren Sie betroffene Geräte so weit wie möglich, um eine weitere Verbreitung zu verhindern.

Wenn Ransomware zuschlägt, ist es wichtig, die betroffenen Geräte so weit wie möglich zu isolieren, um eine weitere Verbreitung zu verhindern. Gehen Sie davon aus, dass die Angreifer zum Zeitpunkt des Ransomware-Angriffs bereits gut in Ihre Umgebung integriert sind, sodass schnelles Handeln zur Eindämmung der Auswirkungen entscheidend ist.

Isolieren Sie zunächst die infizierten Geräte und entfernen Sie sie aus dem Netzwerk. Ziehen Sie die Netzwerkkabel ab, unterbrechen Sie die Netzwerkverbindungen (einschließlich WiFi-Netzwerke).

Wenn Ihr Netzwerk dies zulässt und ordnungsgemäß segmentiert ist, können Sie das infizierte Netzwerksegment auch abtrennen.

Schalten Sie die infizierten Geräte NICHT aus und vermeiden Sie das Herunterfahren der Systeme. Es könnte noch Malware installiert sein, die nicht aktiviert ist. Ein laufendes System kann auch hilfreich sein, wenn Sie ein Unternehmen für die Reaktion auf Vorfälle um Hilfe bitten, um detaillierte Untersuchungen durchzuführen.

Beginnen Sie keine Wiederherstellungsmaßnahmen, solange das Ausmaß des Angriffs nicht bekannt ist, d. h. die Methode, der Zeitpunkt und die betroffenen Systeme.

3. Einen separaten Kommunikationskanal einrichten

Gehen Sie davon aus, dass Ihre geschäftlichen Kommunikationsmittel (falls noch funktionsfähig) beeinträchtigt sind.

Sensible Mitteilungen über die Entwicklung des Vorfalls sollten über einen getrennten und gesicherten Kanal erfolgen. Gehen Sie davon aus, dass auch Ihre Mailsysteme (sofern noch funktionsfähig) angegriffen wurden und der Angreifer Zugang zu diesen Systemen hat, was bedeutet, dass die Kommunikation in Ihrem Netz auf das absolute Minimum beschränkt werden sollte. Analysieren Sie, welche Systeme für die interne und externe Kommunikation genutzt werden könnten. Richten Sie einen sicheren Kommunikationskanal mit Ihrem technischen Team und dem Führungsteam ein.

Es ist ratsam, z. B. ein Signal oder vorübergehend ein externes Konferenzsystem (sicheres Kommunikationstool) zu verwenden und getrennte Gruppen zu bilden. Vielleicht möchten Sie eine Gruppe mit den technischen Verantwortlichen, eine Gruppe mit den Kommunikationsverantwortlichen und eine Gruppe für die Führung einrichten. Die Hälfte der Arbeit bei der Bewältigung eines Ransomware-Vorfalls besteht in der Koordination und Kommunikation.

4. Einrichtung eines Krisenmanagementteams

Das Krisenmanagementteam koordiniert alle Aktivitäten, die erforderlich sind, um Ihre IT-Systeme wieder betriebsbereit zu machen, kümmert sich aber auch um geschäftliche, IT-Prioritäten, Kommunikation und rechtliche Aspekte.

Bilden Sie ein Krisenmanagementteam (manchmal auch als Business-Continuity-Team bezeichnet), das sich mit Geschäftsfachleuten, Kommunikationsstrategien und rechtlichen Fragen befasst und bei der Lösung von Prioritätenkonflikten hilft, wenn die Wiederherstellung von Geschäftsfunktionen in Angriff genommen werden muss.

Dieses Team sollte die gesamte interne und externe Kommunikation koordinieren und sicherstellen, dass während der Krise "eine Stimme" verfügbar ist.

Dem Krisenmanagementteam sollten die wichtigsten Interessengruppen des Unternehmens, Ihr DSB, die Kommunikationsabteilung, die Rechtsabteilung und ein IT-Vertreter angehören.

Ernennen Sie einen Krisenmanager, der als Bindeglied zwischen Ihrem(n) technischen Team(s) und dem Krisenmanagementteam fungiert.

Je nach Größe des Unternehmens können Sie zwei Krisenmanagementteams in Betracht ziehen, eines für die geschäftlichen Aspekte und eines für die operativen IT-Aspekte (wobei letzteres direkt an das geschäftliche Krisenmanagement berichtet).

5. Aktivieren Sie Ihr Reaktionsteam für Cybervorfälle

Holen Sie sich professionelle Hilfe von Cyberspezialisten, z. B. Forensikern, die Ihnen dabei helfen können, herauszufinden, wie es zu dem Vorfall gekommen ist, und eine Wiederholung zu verhindern.

Prüfen Sie, ob die Reaktion auf Vorfälle Teil Ihres Versicherungsvertrags ist.

Prüfen Sie, ob Sie über internes Fachwissen verfügen, oder beauftragen Sie andernfalls ein professionelles Incident-Response-Team, das Sie bei der Bewertung des ursprünglichen Angriffsvektors und des Eintrittspunkts unterstützt und eine angemessene Schadensbegrenzung ermöglicht.

6. Frühzeitig und häufig kommunizieren

Kommunizieren Sie frühzeitig und häufig, halten Sie Ihre internen Mitarbeiter, Lieferanten, Dienstleister und Ihre Kunden auf dem Laufenden. Diesen Angriff zu verheimlichen ist generell keine gute Idee, da er dem Ruf Ihrer Marke schaden kann.

Seien Sie gegenüber Ihren Mitarbeitern, Interessenvertretern, Kunden oder Nutzern und der Presse so transparent wie möglich über den Angriff. Auch wenn Sie noch nicht alle Antworten kennen, ist es wichtig, alle Beteiligten zu informieren. Weitere Informationen: https://www.cert.be/en/crisis-communication-event-cyber-attack.

Wenn Ihre Kommunikationssysteme nicht verfügbar sind, ziehen Sie bitte vorübergehende Lösungen in Betracht, wie z. B. die Einrichtung einer Kommunikationswebseite oder SMS-basierte Massenbenachrichtigungssysteme.

7. Erledigen Sie Ihre rechtlichen Verpflichtungen

Ransomware-Akteure sind nicht nur daran interessiert, dass Sie das Lösegeld zahlen, um die Systeme zu entschlüsseln, sondern haben oft auch Daten exfiltriert und drohen damit, sie zu verkaufen oder öffentlich zugänglich zu machen, wenn Sie nicht zahlen.

Es gibt gesetzliche Verpflichtungen zur Benachrichtigung von Behörden wie der DPA/GBA/APD bei Verdacht auf Datenschutzverletzungen (in der Regel innerhalb von 72 Stunden). https://www.gegevensbeschermingsautoriteit.be/burger/acties/contact (Website in NL und FR verfügbar). Beziehen Sie Ihren Datenschutzbeauftragten (DSB) ein.

Das Rechtsteam und/oder der DSB können auch eine Anzeige bei der örtlichen Polizei erstatten.

8. Bewerten Sie die Integrität Ihrer Backups

Vergewissern Sie sich, dass die Angreifer nicht auch die Sicherheit und Integrität Ihres Backup-Systems beeinträchtigt haben.

Wenn das Sicherungssystem sicher ist, d. h. Sie über eine unabhängige und überprüfte Kopie Ihrer Daten verfügen, ist die Vermeidung von Lösegeldzahlungen die empfohlene und beste Option. Daher sollten Sie eine Bestätigung haben, dass die Backups nicht kompromittiert wurden oder kein Zugriff erfolgt ist (unveränderliche Backups sind ein Muss).

9. Koordinieren Sie Ihre Reaktion auf die Hacker

Grundsätzlich sollten Sie KEIN Lösegeld an kriminelle Organisationen zahlen.

Das CCB (Centre for Cybersecurity Belgium) rät dringend von der Zahlung eines Lösegelds ab. Es kann Situationen geben, in denen die Zahlung die einzige verbleibende Option ist, aber bitte bedenken Sie, dass die Angreifer sehr wahrscheinlich an finanziellem Gewinn interessiert sind, so dass alle Gelegenheiten, mehr Geld zu erpressen, von diesen Akteuren bewertet werden.

Seien Sie vorsichtig, wenn Sie mit dem Angreifer verhandeln. Die Beauftragung eines professionellen Unterhändlers ist kein Patentrezept. Es sind viele Fälle bekannt, in denen Lösegeldbeträge verdoppelt wurden, nachdem ein Unterhändler engagiert wurde, und denken Sie immer daran, dass es keine Garantie dafür gibt, dass Sie die Entschlüsselungsschlüssel erhalten werden.

10. Umsetzung von Minderungsmaßnahmen

Implementierung von (minimalen) Sicherheitsüberwachungsdiensten (SOC-Dienst), Aktivierung einer Endpunkt-Erkennung. Patchen, Zurücksetzen, Aktualisieren bekannter anfälliger Systeme, die von dem Angriff betroffen sind. Implementierung einer Multi-Faktor-Authentifizierung.

Öffnen Sie die Internetverbindung nicht für alle Benutzer, sondern konzentrieren Sie sich zunächst auf die Benutzer, die für die Wiederherstellung des IT-Betriebs Ihrer Krisenmanagementfunktionen erforderlich sind.

Patchen, Zurücksetzen, Aktualisieren bekannter anfälliger Systeme, die von dem Angriff betroffen sind. Führen Sie einen vollständigen Reset aller Passwörter durch und implementieren Sie, falls noch nicht geschehen, eine Multi-Faktor-Authentifizierung. Konzentrieren Sie sich zunächst auf privilegierte Konten und Dienste (Admin-Konten, Admin-Dienste).

Implementieren Sie Sicherheitsüberwachungsdienste (SOC-Service), aktivieren Sie eine Endpunkt-Erkennungslösung für die kritischen Systeme wie die Authentifizierungs- und Autorisierungssysteme und die Systeme, die mit dem Internet verbunden sind. Der Punkt ist, dass Sie einen (besseren) Überblick über die Aktivitäten in Ihrem Netzwerk haben wollen.

11. Beginnen Sie mit dem Wiederaufbau Ihrer Systeme

Patchen, Aktualisieren, Wiederherstellen und Zurücksetzen Ihres Authentifizierungssystems, Implementierung der Multi-Faktor-Authentifizierung

Stellen Sie ein System nicht auf der Grundlage von Backups kurz vor oder nach dem Angriff wieder her.

Führen Sie zuerst die oben genannten Punkte aus und beginnen Sie erst dann mit der Wiederherstellung Ihres Systems anhand von Sicherungskopien.

Achten Sie darauf, saubere Systeme während der Wiederherstellung nicht erneut zu infizieren. Sobald das System wiederhergestellt ist, sollten Sie es überprüfen, um sicherzustellen, dass sich keine bösartigen Inhalte mehr darauf befinden, bevor Sie es wieder in Ihr Netzwerk einbinden. Stellen Sie Ihre Systeme auf der Grundlage einer Prioritätenliste der kritischen Dienste wieder her; stellen Sie zuerst die Server und dann die Endpunkte wieder her. Es wird auch empfohlen, eine Kopie der verschlüsselten Daten aufzubewahren, da in Zukunft möglicherweise ein kostenloses Entschlüsselungstool für den Ransomware-Stamm zur Verfügung stehen wird.

Entfernung oder vollständige Isolierung von Altsystemen und -protokollen.

12. Überprüfung und Hinzufügung zusätzlicher Schutzmaßnahmen zur Verhinderung künftiger Angriffe

Während der Schwerpunkt auf der Beseitigung des Angriffs und dem Wiederaufbau der Infrastruktur liegt, muss sich die Unternehmensführung darüber im Klaren sein, dass es möglich ist, erneut angegriffen zu werden.

Nehmen Sie sich die Zeit, den Angriff im Detail zu analysieren und zu dokumentieren, neue Kontrollen, Prozesse, Verfahren und Lösungen einzuführen, um einen erneuten Angriff zu verhindern.

Webinar auf Niederländisch und Französisch verfügbar: https://www.youtube.com/watch?v=r0Iraugn-wo

Die Ransomware-Broschüre von CERT.be ist auf Niederländisch und Französisch verfügbar.

Haftungsausschluss

Dieses Dokument und seine Anhänge wurden vom Zentrum für Cybersicherheit Belgien (CCB) erstellt, einer föderalen Verwaltung, die durch den Königlichen Erlass vom 10. Oktober 2014 geschaffen wurde und dem Premierminister untersteht.

Die CCB übernimmt keine Verantwortung für den Inhalt dieses Dokuments.

Die bereitgestellten Informationen:

- sind ausschließlich allgemeiner Natur und zielen nicht darauf ab, alle besonderen Situationen zu berücksichtigen;

- sind nicht notwendigerweise in allen Punkten erschöpfend, präzise oder auf dem neuesten Stand.

Verantwortlicher Herausgeber

Zentrum für Cybersicherheit Belgien

Herr De Bruycker, Direktor

Rue de la Loi, 16

1000 Brüssel