BDO CYBER SECURITY

VULKAN FILES:
WIR WISSEN JETZT, WAS WIR EIGENTLICH SCHON WUSSTEN
04.04.2023

Die deutsche Wirtschaft muss die Cyber-Bedrohungslage ernst nehmen und handeln. Zehn Handlungsempfehlungen, um vorbereitet zu sein.

Am 30. März 2023 berichten die Medien über die Enthüllung der sogenannten Vulkan-Files, eine Reihe von internen Unterlagen der russischen IT-Sicherheits- und Softwarefirma NTC Vulkan aus den Jahren 2016-2021. Diese decken Informationen zu Cyberwaffen auf, welche einen längst begonnenen und durch Russland geführten Cyberkrieg offensichtlich erscheinen lassen.

Die Fakten der Pressemitteilungen lesen sich wie ein Agenten-Thriller. Es ist die Rede von Schadsoftware, welche Computersysteme eines Flughafens lahmlegen, Zugentgleisungen auslösen und die Stromversorgung unterbrechen können, so der Spiegel. Es geht um die Kontrollsysteme unserer kritischen Infrastruktur. Im Visier seien konkret Eisenbahn-, Luft- und Schiffstransport sowie Energieunternehmen. Die Politik spricht von „Cyberwaffen“ und „Cyberkrieg“.

Der bittere Ernst der Sache lässt sich jedoch nicht mehr ausblenden. Schaut man nüchtern auf die Sicherheitslage deutscher Unternehmen, zeichnet sich ein düsteres Bild. Der Staat ist zu langsam. Unternehmen wägen sich weiterhin in der Hoffnung, nicht getroffen zu werden. Wieviel dabei auf dem Spiel steht, können Entscheidungsträger oft für ihr eigenes Unternehmen nicht erfassen.

„Nach meiner Kenntnis ist Vulkan nicht die einzige Firma, die mit den russischen Nachrichtendiensten kooperiert. Offensichtlich haben viele Politiker und Entscheidungsträger immer noch nicht verstanden, dass wir ein Angriffsziel u.a. russischer Cyberaktivitäten sind. Nicht nur - aber gerade besonders - in Kriegszeiten.“, Bernd König, Cyber-Experte und IT-Sachverständiger im Ring deutscher Gutachter e.V.

MIT DIGITALER KRIEGSFÜHRUNG KONFRONTIERT

Mit den Vulkan-Files ist nun bestätigt, wovon bereits lange ausgegangen werden musste. Cyberangriffe sind und werden zunehmend Teil der Kriegsführung. Dabei wird mit Schadprogrammen zum Ausspionieren von Daten, zwecks Überwachung und für das Eindringen und Lahmlegen von IT- und Kontrollsystemen aufgerüstet. Die Vergangenheit hat bereits eindrucksvoll dargestellt, dass die Manipulation von Wahlen, die Störung der Stromversorgung, das Verteilen von Desinformationen und der Angriff auf Atomkraftwerke möglich sind.

Dahinter stecken Hackergruppen bis hin zu Softwarefirmen, die teilweise im Auftrag der Geheimdienste arbeiten, wie es bei der Firma NTC Vulkan und ihren Verbindungen zum militärischen, inländischen und ausländischen Geheimdiensteinheiten Russlands (GRU, FSB und SVR) der Fall zu sein scheint.

„Die Vulkan-Files sind endlich eine Bestätigung dessen, was ich seit einigen Jahren meinen Studierenden in der Vorlesung als Vermutung erkläre: Die Grenzen zwischen den russischen Diensten und den kriminellen Gruppen sind fließend. Als deutsches Unternehmen, das von einem Ransomware-Angriff betroffen ist oder war, muss man aus meiner Sicht davon ausgehen, dass die Firmendaten auch kopiert und ausgewertet werden. Alles andere wäre blauäugig.“, sagt Prof. Dr. Alexander Schinner an der Hochschule für angewandte Wissenschaften Würzburg-Schweinfurt.

ÜBER BDO CYBER SECURITY

BDO Cyber Security ist Ihr Berater und Anbieter ganzheitlicher Lösungen rund um die IT- und Informationssicherheit. Unsere Kernkompetenzen sind Identity and Access Management, Compliance nach gängigen Standards sowie die Etablierung und Betrieb von Managementsystemen (ISMS). Das hauseigene Security Operations Center (SOC) mit 24/7-Betrieb, Incident Response Teams runden das Portfolio ab.

www.bdosecurity.de

KONTAKT

BDO Cyber Security GmbH

FRANZISKA HAIN
BDO Cyber Security GmbH
Geschäftsführerin
Tel.: +49 152-56012793
franziska.hain@bdosecurity.de

ANDREAS STEMICK
BDO Cyber Security GmbH
Geschäftsführer
Tel.: +49 211 1371331
andreas.stemick@bdodigital.de

WO STEHEN WIR IN DEUTSCHLAND?

Vom Bundesamt für Sicherheit in der Informationstechnik (BSI) heißt es noch im Bericht zur Lage der IT-Sicherheit in Deutschland für 2022: „Bislang gab es in Deutschland in Zusammenhang mit dem Angriffskrieg Russlands gegen die Ukraine eine Ansammlung kleinerer Vorfälle und Hacktivismus-Kampagnen. [..] Eine übergreifende Angriffskampagne gegen deutsche Ziele war nicht ersichtlich. Die Lage im Cyber-Raum von NATO-Partnern war dagegen teilweise angespannt und in der Ukraine teilweise existenzbedrohend kritisch." Man sah sich bisher nur mit Kollateralschäden grundsätzlich bedroht. Am 31. März stuft Bundesinnenministerin Faeser nun in einem Interview gegenüber dem Spiegel die Gefahr als sehr hoch ein.

Ein in Bezug auf die Folgen eindrucksvolles Beispiel aus 2022 gibt es dennoch. Der Cyberangriff auf eine Landkreisverwaltung in Sachsen-Anhalt führte zum Ausruf des Katastrophenfalls. „Bürgernahe Dienstleistungen waren über 207 Tage lang nicht oder nur eingeschränkt verfügbar." So schreibt das BSI.

Der Lagebericht verzeichnet 15 Millionen Meldungen zu Schadprogramm-Infektionen im Jahr 2022 in Deutschland. Diese Größe wirkt kraftvoll.

Laut einer Studie[1] verursache ein erfolgreicher Hacker-Angriff auf ein Großunternehmen einen durchschnittlichen wirtschaftlichen Schaden von 1,8 Millionen Euro. Bei kleinen und mittelständischen Unternehmen läge der Durchschnittswert im Jahr 2022 bei 193.697 Euro.

Die Herausgeber von Cyberversicherungen jedoch verhalten sich in den letzten Jahren zögerlich. Das Cyber-Risiko wird als eine der sich am schnellsten entwickelnden Risikoarten verstanden. Keine gute Voraussetzung, um ökonomisch sinnvolle Prämien anzusetzen. Nicht zuletzt vor diesem Hintergrund wird die Versicherbarkeit und deren anzusetzenden Kriterien der Risiko-Quantifizierung seit geraumer Zeit diskutiert.

WAS IST ZU TUN?

Zeit spielt eine kritische Rolle. Wie ist seit Jahren etablierten Hackergruppen und lang vorbereiteten Angriffs-Strategien jetzt zu begegnen? Wie den automatisiert ablaufenden Softwareprorammen und KI-gestützten Algorithmen nicht ins Netz gehen? Ein fatales Wortspiel.

Dort wo grundlegende technische und organisatorische Sicherheitsmaßnahmen sowie präventiv und wirksam ausgearbeitete Handlungsstrategien für den Ernstfall fehlen, wird der Faktor Zeit zur Herausforderung.

Gleichzeitig bestehen Möglichkeiten, strukturiert und mit wenigen Mitteln einen relevanten Schritt auf dem Weg zu einer Cyber Resilienz zu erzielen.

Dabei gilt grundsätzlich, Vertrauen in ein Messen, Kontrollieren und Überprüfen umzuwandeln. Wer jetzt noch auf Vertrauen setzt, dürfte nicht mehr lange gut bedient sein. Es gibt keinen Grund, warum nicht auch Cloud Provider, IT-Dienstleister und Zulieferer ebenfalls auf dem Radar der Angreifer stehen dürften.

Die stetige Kontrolle der Informationssicherheit sowie messbare Kriterien zur Einschätzung des Sicherheitsniveaus für Entscheidungsträger dürfen nicht mehr auf sich warten lassen.

Im Folgenden finden Sie zehn priorisierte Handlungsempfehlungen.

ZEHN HANDLUNGSEMPFEHLUNGEN

1. Managed Detection & Response (MDR)

Es gilt, eine Echtzeitüberwachung des Netzwerkes eine rund um die Uhr (24/7) sicherzustellen.
Das Ziel vieler Angriffe sind insbesondere Netzwerk-Endpunkte. Managed Detection- und Response-Services bieten eine Automatisierungs- und Überwachungsfunktion. Mit dem Einsatz von state-of-the-art Technologien und mit Hilfe von Triage und Empfehlungen, Erstellen und Aktualisieren von Inhalten, Korrelation von Alarmen und forensischen Funktionen untersucht der MDR-Service sogenannte Events (Alarme, Abweichungen, Auffälligkeiten im Netzwerk-Verkehr).

2. IT-Incident Response

Der Ablauf zum Erkennen, Einstufen, Alarmieren und Behandeln eines kritischen IT-Incidents ist in einem Incident Response Prozess präventiv festzulegen. Dabei gilt es, die notwendige Kompetenz handelnder Personen sicherzustellen. Fehlt das Knowhow im eigenen Unternehmen, können mittels sogenannter Retainer-Verträge mit Incident Response-Anbietern Unterstützungsleistungen für den Einsatzfall vorgehalten werden. Wird derartiger Support erst im Fall des Cyberangriffs eingekauft, sind Betroffene meist in Bezug auf die Vergütung im Nachteil.

[1] „CyberDirekt Risikolage 2022" vom 28. März 2022

3. Krisenmanagement

Der Cyberangriff ist fast immer für Betroffene eine Situation, die von Überforderung, Emotionen, Aktivismus und Zeitnot geprägt ist. Auch hier gilt es, ein Krisenmanagementprozess präventiv zu planen und sogar auf Wirksamkeit zu testen. Legen Sie fest, welche Stakeholder im Ernstfall zusammenkommen und welche Möglichkeiten der Kommunikation auch beim Ausfall der IT genutzt werden können. Beziehen Sie den Austausch mit Mitarbeitern, Kunden, Dienstleistern und Presse ein.

4. Kontakt zur Strafverfolgung

Nehmen Sie schon jetzt Kontakt mit den für Sie zuständigen Strafverfolgungsbehörden auf. Informieren Sie sich, mit welcher Unterstützung Sie rechnen können. In der Regel treffen Sie hier auf erfahrene Beamte, denen z.B. der Erpressungsfall mittels Ransomware geläufig ist.

5. Transparenz mittels Business Impact Analyse

Schaffen Sie unbedingt Transparenz zu den Abhängigkeiten Ihrer Geschäftsaktivitäten von der IT. Durchdenken Sie das Fortsetzen des Geschäftsbetriebs gänzlich ohne IT. Ermitteln Sie kritische Geschäftsprozesse und Ressourcen und priorisieren Sie deren Aufnahme eines Notbetriebs sowie die Wiederherstellung des Originalzustands. Beziehen Sie dabei Ihre Lieferketten sowie Dienstleister (IT, Strom, Logistik, etc.) mit ein.

6. Cloud Provider prüfen

Haben Sie Cloud-provider im Einsatz, vertrauen Sie nicht auf deren Leistungen ohne Nachweis. Haben Sie im Blick, welche Daten in welcher Form und von wem in der Cloud verarbeitet werden und überprüfen Sie vereinbarte Sicherheitsleistungen selbst oder durch einen unabhängigen Auditor.

7. Szenarien simulieren

Eine einfache Übung ist das Erstellen einiger kritischer Cyberangriffs-Szenarien. Nutzen Sie diese, um mit relevanten Stakeholdern die Situation „durchzuspielen". Die Was-wäre-wenn-Frage bringt Sie zu brauchbaren Erkenntnissen, offenbart offene Flanken und verbindet Stakeholder für den Ernstfall.

8. Notfallplanung erstellen

Erstellen Sie für Ihre kritischen Geschäftsaktivitäten eine Notfallplanung, welche auf einem Handeln ohne IT basiert. Dabei ist der Fokus nicht nur auf die IT selbst, sondern auch auf das IT Service Continuity Management zu legen. Während die IT an der Wiederherstellung der IT-Systeme arbeitet, müssen kritische Prozesse weitergeführt werden.

Beachten Sie in der Notfallplanung unterschiedliche Ausfallzeiten der IT. Je nach Schweregrads des Cyberangriffs können die forensische Untersuchung und Wiederherstellung der IT Tage und Wochen in Anspruch nehmen.

9. Threat Intelligence Informationen beziehen

Um die Risikolage für Ihr Unternehmen beurteilen zu können, empfiehlt es sich, auf sogenannte Threat Intelligence Informationen zurückgreifen zu können. Diese sind über entsprechende Anbieter zu beziehen und sollten im internen Risikomanagement regelmäßig verwertet werden.

10. Technisch nachrüsten

Unterziehen Sie die technischen Aspekte Ihrer Informationssicherheit einer schonungslosen Überprüfung und entscheiden Sie, welche Investition für die Sicherung Ihrer Unternehmenswerte notwendig sind.

Cyberkriminalität hat sich mit ihrer komplexen Facette zu einem wirkungsvollen und fast schon zuverlässigen Unternehmensrisiko etabliert und ist seitens der Angreifer ein etabliertes und effektives Geschäft. Cybercrime-as-a-service - die Straftat im digitalen Raum als Dienstleistung - so wie sie eben Russland zu beauftragen scheint, wird die deutsche Wirtschaft noch lange wachhalten.

Bleiben Sie daher ungeduldig auf dem Weg zu Ihrer Cyber-Resilienz und sprechen Sie uns an!

Die Informationen in dieser Publikation haben wir mit der gebotenen Sorgfalt zusammengestellt. Sie sind allerdings allgemeiner Natur und können im Laufe der Zeit naturgemäß ihre Aktualität verlieren. Demgemäß ersetzen die Informationen in unseren Publikationen keine individuelle fachliche Beratung unter Berücksichtigung der konkreten Umstände des Einzelfalls. BDO Cyber Security übernimmt demgemäß auch keine Verantwortung für Entscheidungen, die auf Basis der Informationen in unserenPublikationen getroffen werden, für die Aktualität der Informationen im Zeitpunkt der Kenntnisnahme oder für Fehler und/oder Auslassungen.

BDO Cyber Security GmbH, eine Gesellschaft mit beschränkter Haftung deutschen Rechts, ist Mitglied von BDO International Limited, einer britischen Gesellschaft mit beschränkter Nachschusspflicht, und gehört zum internationalen BDO Netzwerk voneinander unabhängiger Mitgliedsfirmen.
BDO ist der Markenname für das BDO Netzwerk und für jede der BDO Mitgliedsfirmen.

© BDO Cyber Security.

BDO CYBER SECURITY