Leitfaden für den erfolgreichen Schutz gegen Cyberkriminalität

Oktober 2021

Cyberkriminalität oder Cybercrime kann jedes Unternehmen und Organisation treffen. Fast täglich gibt es Meldungen von Firmen, die Opfer einer Cyberattacke wurden[1]. Neuralgische Punkte sind dabei unter anderem:

1. Oft dauert es Wochen, bis die betroffene Firma oder die öffentliche Verwaltung merkt, dass deren Systeme gehackt wurden[2] .
2. Hacker Angriffe erfolgen dieser Tage vermehrt nicht mehr über E-Mails, die Schadsoftware enthalten und beim anklicken durch Nutzer aktiviert werden. Vielmehr verschaffen sich Hacker über Schwachstellen direkt Zugang zu vertraulichen Daten[3].
3. Im Schnitt dauert es oft mehr als 100 Tage, bis bekannte kritische Schwachstellen in Systemen gefixt wurden. Das erhöht[4] die Verletzbarkeit und die Möglichkeit eines Diebstahls von Daten.

Versicherer haben aus **Risikomanagement-Gründen** deren Prämien für die Versicherung gegen Schäden durch Cyberkriminalität in den letzten 12 Monaten um etwa 30 bis 40% erhöht. Trend weiterhin steigend.

Gemäss Maya Bundt von Swiss Re[5] (Head Cyber- und Digital Solutions) braucht eine Firma gut 3 Wochen nach einem Angriff, bis sie wieder vollständig produktiv ist. Ebenfalls kostet es wertvolle Ressourcen, bis der Vorfall verarbeitet ist, bis die IT-Forensik die Wiederherstellung der Daten und Systeme geschafft hat.

Vorbeugen ist also wichtig, um das Risiko, Opfer einer Cyber-Attacke zu werden, zu minimieren. Definitiv auch kostengünstiger, als nach einer Attacke das Problem lösen zu müssen. Noch dazu möglicherweise Lösegeld zu zahlen, Reputationsschaden hinnehmen zu müssen und bei Kunden Vertrauen zu verlieren.

Das rechtzeitige **Identifizieren und Ausmerzen von Schwachstellen wird immer wichtiger**. Dabei ist es notwendig, dass Nutzer und ethische Hacker solche Schwachstellen melden können, ohne dabei negative Folgen für sich zu fürchten (siehe z.B. CSU 2021 Wahl App[6]).

info@drkpi.com +41 44 2721876 CyTRAP Labs GmbH Röntgenstrasse 49 CH-8005 Zürich

Die Lösung für das optimale Risikomanagement ist ein **Vulnerability Disclosure Programm (VDP)**, das wir hier vorstellen.

Erstellen der Leitlinien für ein VDP

Zunächst sollte die Leitlinie, auch Policy, zur Durchführung des Programms zur Schwachstellenmanagement aufgesetzt werden.

In der Policy werden Strukturen, Abläufe und das **Prozessmanagement** für die von Hackern oder Reportern eingereichten Schwachstellen festgelegt. Ebenfalls spielt Compliance eine Rolle. Dafür braucht es eine Beschreibung des VDP für partizipierende Hacker, in dem Richtlinien festgelegt werden,

- welche Systeme Teil des Programms sind,
- was Hacker unternehmen dürfen und was nicht und
- Nennung der Systeme, welche “in scope” und “out of scope” sind.

Ein effektives VDP und die regelmässige Überprüfung der Risiken wird die Wahrscheinlichkeit eines erfolgreichen Hackerangriffs um etwa 45 - 60% reduziert. Dies spart Ressourcen und Kosten, welche z.B. nach einem erfolgreichen Hackerangriff bei einem 2 Woche dauernden Produktionsausfall anfallen. Es baut aber ebenfalls das Vertrauen der Kunden in die Applikationen des Unternehmens auf.

Ein **VDP ist ein wichtiger Bestandteil für das Compliance-Programm**. Es **kommuniziert nach aussen wie auch innen**, dass Informations- und Datensicherheit für die Firma oder Verwaltung wichtig sind.

info@drkpi.com +41 44 2721876 CyTRAP Labs GmbH Röntgenstrasse 49 CH-8005 Zürich

VDP: Schlüsselelemente und Best Practice

5 Schlüsselelemente

VDPs müssen nicht lang sein, enthalten aber im Allgemeinen **fünf Schlüsselelemente**:

1. **Versprechen**: Zeigen Sie eine klare, gutgläubige Verpflichtung gegenüber Kunden und anderen Stakeholdern, die potenziell von Sicherheitslücken betroffen sind.
2. **Umfang**: Geben Sie an, welche Eigenschaften, Produkte und Schwachstellenarten abgedeckt sind.
3. **Sicherheit für den Schwachstellen-Melder**: Stellt sicher, dass gutgläubige Melder nicht bestraft werden (siehe Beispiel Lilith Wittman[6]).
4. **Prozess**: Der Prozess definieren, den Melder verwenden, um Schwachstellen zu berichten z.B. über ein Webformular und/oder auch eine E-Mail Adresse.
5. **Präferenzen**: Die Policy ist ein lebendes Dokument, das Erwartungen für Präferenzen und Prioritäten hinsichtlich der Bewertung von Meldungen festlegt.

Best Practice Faktoren

Gemäss Best Practice in den USA werden von einem VDP drei Dinge erwartet[7].

1. Die erste Komponente ist ein **offenes Programm**, bei dem die Öffentlichkeit Schwachstellen in IT-Systemen finden und melden kann. Dies kann z.B. über ein Formular auf der Website der Firma oder Verwaltung geschehen. Hier kommt es auf den “Good Will” an, d.h. der rapportierende Hacker (der Samariter) erhält eigentlich keine Belohnung für dessen Arbeit.
2. Zweite Komponente ist das **Bug-Bounty Programm**. Dies ist ein Programm, bei dem Spezialisten dafür bezahlt werden, Schwachstellen zu finden. Es ist in 80% der Fälle privat, d.h. Hacker werden eingeladen teilzunehmen.
3. Die dritte Komponente sind **Penetrationstests**. Hier werden interne oder externe Teams (beispielsweise das SOC-Team) mögliche Wege zum Angriff auf Systeme simulieren.

info@drkpi.com +41 44 2721876 CyTRAP Labs GmbH Röntgenstrasse 49 CH-8005 Zürich

Nachhaltige Überprüfung des Risikos

Ein Vulnerability Disclosure Programm (VDP) ist ein wichtiger Schritt, um sich gegen Cyberkriminalität zu schützen. Um Risiken und mögliche Schäden durch Datenverlust, Datenmanipulation oder Datenschutzverletzungen zu verringern, sind die folgenden 4 Schritte neben der Einführung des VDP umzusetzen.

1. Funktionierende Backups

Gut funktionierende **Backup-Infrastrukturen** sind effektive Prozesse, Kontrollen und gut überlegte Datenlagerung. Dateibasierte Umgebung mit Cloud-basiertem Schutz oder die Unternehmungsanwendung auf mehreren Servern können komplexe Datenabhängigkeiten aufweisen. Dies erfordert eine **Backup-Synchronisation**, um eine brauchbare Wiederherstellung zu bekommen. Die Brauchbarkeit dieser Backups muss regelmässig überprüft und eingestellt werden (siehe Fire Drill). Best Practice ist hier täglich ein inkrementelles Backup und mindestens jeden Monat oder halbjährlich ein Voll-Backup durchzuführen[9]. Diese Backups sind natürlich separat gespeichert und weder über das Internet noch intern frei zugänglich.

2. Notfallplan (Business Continuity Plan)

Ohne eine gut durchdachte und erprobte Notfallplanung ist ein koordiniertes und zielführendes Handeln der Beteiligten im Ernstfall aller Erfahrung nach eher unwahrscheinlich. Beispielsweise beinhaltet der **Wiederherstellungsplan** alle durchzuführenden Tätigkeiten und Massnahmen, die nach einem IT-Ausfall oder einem Cyber-Security-Vorfall zu ergreifen sind. Er identifiziert **Verantwortlichkeiten**, definiert **Eskalationswege** und berücksichtigt die verschiedenen Ausfallszenarien (z.B. langes Wochenende). Natürlich braucht es auch ein **Disaster-Recovery-Team**, um die Wiederherstellung der System z.B. dank funktionierender Backups rasch zu gewährleisten.

3. Kennzahlen, Benchmarks: Zielsetzung

Für das VDP und Cyber-Risikomanagement braucht es vorher definierte Kennzahlen.. **Quantitative Metriken** sind z.B. innerhalb wievieler Tage Software-Patches oder Schwachstellen mit der höchsten Risikostufe eingespielt werden.

info@drkpi.com +41 44 2721876 CyTRAP Labs GmbH Röntgenstrasse 49 CH-8005 Zürich

Geschäftsrelevante Metriken helfen das Risiko für wichtige Anwendung wie ein e-Shop zu minimieren. Direkte Kosten (e-Shop steht still) und indirekte Kosten (Logistikarbeiter hatten nichts zu tun) wegen einer Hacker Attacke sind hier für die Geschäftsleitung von Interesse.

4. Fire Drill

Dient der laufenden Überprüfung der aufgesetzten Massnahmen und soll als Folge die **Verbesserung der Effizienz der Prozesse** haben. Die IT ist ständig in Bewegung und es ist fraglich, ob nach einiger Zeit noch alle Massnahmen greifen. Deshalb sind z.B. regelmässige Disaster-Recovery-Tests/Fire Drills nötig. Sie zeigen, ob die Planung und Prozesse angepasst werden müssen und inwiefern die Backups es erlauben, IT Systeme innerhalb kurzer Zeit wieder zu 100 % herzustellen.

Warnung

Ransomware wird vermehrt nicht direkt bei der betroffenen Firma aber über z.B. einen Lieferanten, Kunden oder Sicherheitsanbieter eingeschleust[8]. Ein Vulnerability Disclosure Programm mit einem z.B. privaten Bounty-Programm hilft, Schwachstellen zu identifizieren. Doch hilft ein VDP nur dann, wenn die identifizierten Schwachstellen rasch nach Priorität geflickt werden. Das Unternehmen muss auch z.B. einer Versicherung zeigen, dass die Cyber-Risiken nach Best Practice gemanaged werden[10].

Kommunikation

Vorbereitet eine Vorlage zur Kommunikation im Falle eines Hacker-Angriffes. Beispielsweise separat gehostete Website. Diese informiert Stakeholders inkl. Öffentlichkeit/Kunden regelmässig über laufende Aktivitäten im Unternehmen zu Themen wie Datenschutz, Datensicherheit und Cyber-Risiken.

info@drkpi.com +41 44 2721876 CyTRAP Labs GmbH Röntgenstrasse 49 CH-8005 Zürich

Über drkpi®

drkpi® ist eine Division von CyTRAP Labs GmbH. Sie unterstützt Compliance, IT Verantwortliche sowie Geschäftsführerinnen und Geschäftsführer darin, eine starke Cybersecurity Strategie auf- und auszubauen, die zu messbarem Erfolg führt. Wir unterstützen Sie mit umfassender Kompetenz in den Bereichen Vulnerability Disclosure, Cybersecurity, Datenschutz und DSGVO-Compliance. Auch in den Bereichen Content Marketing und SEO, Webdesign und Usability, Corporate Communication und Branding sind wir ein vertrauter Partner für unsere Kunden.

Ressourcen

[1] Auch in der Schweiz und Deutschland sind die Erpresserangriffe gestiegen. Laut Accenture um über 120% (siehe 2021 Threat Report). Sophos fand in einer 2021 Umfrage, dass 31% der Firmen in den letzten 12 Monaten eine Hacker-Attacke hatten, d.h. sie bemerkten diese. Doch die Dunkelziffer ist nicht bekannt (siehe https://twitter.com/InfoSec/status/1433751924231319553)

[2] Die kriminelle Internet-Bande Vice Society hat sich im Mai 2021 Zugang zur Gemeindeverwaltung von Rolle im Kanton Waadt verschafft. Während zwei Monaten hat sie Daten gestohlen. Nachdem die Gemeinde sich weigerte zu zahlen, wurden die Daten ins Darknet gestellt. Die Stadtverwaltung bemerkte angeblich bis im August 2021 nichts davon - siehe https://www.linkedin.com/feed/update/urn:li:activity:6836622450155892736

[3] 2021-09-03 Schweiz Aktuell hat in einer Sendung ein Segment zum Thema Hackerangriffe ausgestrahlt. Der Fokus war auf Endnutzer, welche in E-Mail infizierte Schadsoftware oder Malware anklicken und dadurch Ransomware Attacken Vorschub leistet. Doch die Wahrscheinlichkeit, dass Hacker Zugang vermehrt direkt über nicht eliminierte Schwachstellen und falsche Einstellungen von z.B. Websites, E-Shops, usw. erhalten, wurde von den TV Journalisten und interviewten Experten nicht erwähnt:: https://www.srf.ch/play/tv/redirect/detail/6ae5fc2d-1b57-4fe8-94ee-1cfd07c60a2edd

[4] Gemäss einer 2021 durchgeführten Umfrage von Bitcom mit 1,000 deutschen Unternehmen waren 9 von 10 Unternehmen (88 %) 2020/2021 von Hacker Angriffen - Datendiebstahl, Spionage oder Sabotage - betroffen. In den Jahren 2018/2019 wurden drei Viertel (75 %) Opfer. Dabei dauerte es (siehe 2018/2019 Studie) im Schnitt 170 Tage,

info@drkpi.com +41 44 2721876 CyTRAP Labs GmbH Röntgenstrasse 49 CH-8005 Zürich

bis ein deutsches Unternehmen das Datenleck bemerkte! 170 Tage, in denen sich Hacker ungestört umsehen konnten, nachdem sie es schafften einzudringen: https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr

[5] Maya Bundt von Swiss Re: "Statistiken sagen, dass Unternehmen nach einem Angriff rund drei Wochen brauchen, bis sie wieder vollständig produktiv sind. Wie viel der Ausfall der IT-Systeme kostet, kann man also ausrechnen...und... " https://drkpi.com/de/it-sicherheit-vulnerability-disclosure-programm/#comment-1818

[6] Siehe das Beispiel von Lilith Wittmann, welche Schwachstellen in der CDU Wahl-App fand und dies der Parteizentrale meldete - Details hier inklusive Gesetz - Hacker-Paragraph: https://drkpi.com/de/it-sicherheit-vulnerability-disclosure-programm/#6-die-kommunikation-fuer-millennials-als-schluessel-zum-erfolg (etwas nach unten scrollen)

[7] Congressional Research Service (2020-09-08). Cybersecurity: Recent policy and guidance on Federal Vulnerability Disclosure Programs https://fas.org/sgp/crs/misc/IN11497.pdf

[8] Sie können auch mehr zu diesen Themen auf unseren Seiten lesen. Siehe https://drkpi.com/de/?s=ransomware

[9] Mehr zum Thema: https://anexia.com/blog/de/die-3-besten-backup-strategien/

[10] Je nach System wird es teuer. Ohne einen Audit, welcher der Versicherung zeigt, dass Sie in Sachen Cyber-Risiko Prävention auf dem neuesten Stand sind, wird es schwierig eine Police zu erhalten: https://www.helvetia.com/ch/web/de/geschaeftskunden/kontakt/services/praemienrechner/cyberversicherung-berechnen.html/cyber/risk

info@drkpi.com +41 44 2721876 CyTRAP Labs GmbH Röntgenstrasse 49 CH-8005 Zürich