DrKPI® Cybersecurity

Umsetzung der Cybersecurity Strategie

In 3 Schritten zum besseren Vulnerability und Risiko Management

Sie finden dieses Dokument auch auf unserer Website zum Download:
https://drkpi.com/de/produkt/vulnerability-disclosure-optimiert-tipps-pdf/

Weitere Infos zum Thema hier: https://drkpi.com/de/?p=13478 (Blogeintrag & Download)

Cybersecurity hilft unter anderem das Risiko zu reduzieren, dass unbefugte Nutzer auf das Firmen-Netzwerk zugreifen oder vertrauliche Daten entwenden. Es hilft dem Unternehmen, die Endnutzer, Kunden und Mitarbeitende zu schützen.

Wir präsentieren mit unserem SchnellAudit hier einen **strategischen Ansatz**. Die Beantwortung der hier gestellten Fragen minimiert das **Schadensrisiko von einem Hackerangriff**. Ebenfalls erleichtert unser Ansatz, die negativen Auswirkungen möglichst rasch in den Griff zu bekommen.

Kritisch ist dabei die VDP (Vulnerability Disclosure Program *oder* Policy). Die Basis für ein erfolgreiches VDP ist eine **Richtlinie zur Offenlegung von Sicherheitslücken**. Sie bietet eine klar definierte Möglichkeit und Kanal für jeden, Schwachstellen zu melden.

Das folgende Dokument erläutert die wichtigsten Überlegungen und Aktionen beim Risikomanagement zu Cybersecurity. Es trifft auf Konzerne und Grossfirmen ab ca. 500 Mitarbeitenden zu. Es dient als eine schnelle Einleitung ins Thema mittels einer Checkliste und der Überprüfung des Status Quo.

Ebenfalls ist ein **internes Service Level Agreement (iSLA) zu erstellen**. Dieses definiert, welche Systeme Teil des Programms sind. Welche Standards gesetzt sind. Beispielsweise wie schnell muss eine Schwachstelle mit Priorität 1 gepatcht werden. **Prozesse zur Behebung der Vulnerability** müssen mit dem System Owner definiert sein. Bedeutet, wie funktioniert das genau während einem langen Wochenende (System Owner hat frei von Do-Mo / Ostern). Wer übernimmt (stellvertretend) welche Verantwortung (z.B. System Owner ist krank oder in den Ferien)?

VDPs und Cybersecurity Aktivitäten ganz allgemein müssen gut organisiert sein mit klar definierten Prozessen und Kennzahlen.

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

Schritt 1

Haben Sie die optimalen organisatorischen Strukturen für Cybersecurity Aktivitäten?

Hier stehen die Geschäftsprozesse im Vordergrund, also die Frage, was ist bei Ihnen kritisch? Ebenfalls ist eine schriftliche Fixierung der Pläne, Resultate und Ihrer Antworten notwendig. Die **Strukturen vereinfachen die Ablaufprozesse** und zeigen auf, wer für was, zu welchem Zeitpunkt verantwortlich ist ("Accountability").

In kleineren Teams von 7 oder weniger Mitgliedern ist "free riding" oder ein zurücklehnen und sich rausnehmen für einzelne Personen nicht möglich.

Bitte beantworten Sie die folgenden Fragen.

1. Wurde eine verantwortliche Person für Cybersecurity bestimmt?

Diese Person ist idealerweise Mitglied von oder direkt dem **Vorstand/Geschäftsleitung** unterstellt.

Diese Person ist verantwortlich für das Interne Service Level Agreement (iSLA) und dessen Administration.

2. Existiert eine Steuerungsgruppe Cybersecurity?

Diese setzt Prioritäten und Benchmarks gemäss dem iSLA. Es designed die Prozesse und setzt die Metrics und Benchmarks auf. Beispiel: Wie ist der Zeitrahmen zur Behebung einer Priorität 1 Schwachstelle.

Prozesse und dazugehörende Metrics werden definiert.
Beispiel: Wer wird informiert über die Schwachstelle, Priorität 1. Was passiert wenn nach 1 Std. keine Antwort von dieser Person kommt?

Die Steuerungsgruppe trägt die **Aufsicht** über die Sicherheit der Systeme. Dies gilt auch für die Applikationen, Ressourcen und Daten wie auch für die dazu notwendigen Aktivitäten.

3. Besteht eine zentrale Stelle für Cybersecurity?

Diese ist das ausführende Organ für die von der Steuerungsgruppe aufgestellten Prozesse, Metrics und Verantwortungsbereiche. Die zentrale Stelle verwaltet die Risiken und initiiert die Kontrollen für die Cybersicherheit.

Die Stelle hat eine Matrix Organisation. Dies bedingt, dass z.B. Experten:innen Hot Desking mit der von ihnen bedienten Abteilung machen. Dies fördert die Kommunikation UND reduziert Missverständnisse. Die Experten:innen sind fachlich der verantwortlichen Person Cybersecurity unterstellt.

4. Hat Ihr Unternehmen ein Krisenzentrum für Cybersecurity-Fälle eingerichtet?

Dieses dient der Verwaltung der organisationsweiten Reaktion auf eine Krise im Cybersicherheit Bereich (Cybersecurity Chef:in und die Mitglieder der Steuerungsgruppe sind Teil vom Krisenzentrum). Das Krisenzentrum kommuniziert auch über den Newsblog im Krisenfall nach aussen, wie ersichtlich am Beispiel der T-Mobile von Aug. 2021.

Natürlich lässt sich ohne das notwendige Budget wenig machen. Es gilt die Positionen zu besetzen und die Fachkräfte in den Abteilungen zu integrieren (“embedded cybersecurity experts”). Dadurch kennen sie besser die Bedürfnisse der Abteilungen / Profit Centers und geniessen eine höhere Akzeptanz.

Schritt 2

Wie bereiten Sie sich optimal auf eine Krise vor?

Die beste Vorbereitung ist, wenn **technische Vorkehrungen** helfen, die Risiken von nicht autorisierten Zugriffen zu minimieren. Hier gilt es Risiken gegen Kosten und mögliche Reputationsschäden abzuwägen. Was oftmals bei grossen Vorkommnissen nicht funktionierte, sind diese 3 Punkte, die wir unten aufgeführt haben. Sie sollten überprüfen, wie die Situation in Ihrem Unternehmen ist.

1. Verringerung der möglichen Angriffsflächen der kritischen Systeme

Es gilt für die kritischen Assets deren gesamte Angriffsfläche zu verstehen. Beispielsweise automatische kontinuierlich durchgeführte Schwachstellen-Scans sind empfehlenswert. Sie helfen, unbekannte Legacy Systeme zu entdecken und diese zu patchen oder abzustellen, falls sie nicht mehr gebraucht werden.

Zwei-Faktor-Authentifizierung von Nutzern und regelmässige System Updates sind Pflichtprogramm.

2. Reduktion der Zeitfenster für den Angreifer

Endpunkt-Erkennungs- und Reaktions-Tools, die auf Workstations und Servern installiert sind. Regelmässiges '**Red Teaming**' zur Validierung der Erkennungs- und Reaktionsfähigkeiten = Vulnerability Disclosure Programm, Bug-Bounty Programm - wie schnell werden diese gemeldeten Schwachstellen gepatcht?

Prozesse/Schritte im Falle von Alarm. Beispielsweise an einem langen Wochenende: Wer wird informiert. Was ist akzeptable Reaktionszeit (gemäss iSLA Definition).

Was passiert, wenn z.B. niemand innert 2 Std. intern reagiert. Wird der Prozess automatisch eskaliert? Diese Zusammenhänge müssen von der Steuerungsgruppe mit dem System Owner zusammen definiert werden.

3. Einschränkung oder Begrenzung des Aktionsradius für unbefugten Zugriffs

Wenn Einbrecher:in oder Hacker:in im Haus oder Server eingedrungen ist, muss der **Aktionsradius** drastisch **eingeschränkt** sein. Dadurch werden die Kosten für Attackers erhöht. Es handelt sich beispielsweise um grossen Zeitaufwand und benötigte Rechenkapazität, um weiter zu kommen. Oder wenn komplexe Kenntnisse oder weitere zusätzliche Ressourcen von den Hackergruppen gefordert werden.

Ein Beispiel ist eine **verschlüsselte Datenbank**. Diese kann geknackt werden. Nichtsdestotrotz, wenn diese geknackt ist, sind die Daten im Normalfall immer noch verschlüsselt. Die Hacker müssen also weitere Ressourcen einsetzen, um den Schlüssel zu knacken.

Technische Anpassungen sind zwingend und Best Practice in Sachen Risikomanagement. Als Motivator gilt hier, dass **nur 8% der von einer Ransomware-Attacke betroffenen Unternehmen,** die die Lösegeldsumme bezahlten, danach vollständig ihre verlorenen Daten wiederherstellen konnten.

Auch Umsatzausfälle können gross sein. Bsp. Coop Schweden musste seine Läden für 3-4 Tage im Sept. 2021 schliessen. Hacker hatten das Pay-System gehackt, indem diese sich zuerst Zugang zum Security Provider in Florida verschafften...

Schritt 3

Management von Cybersecurity Vorfällen optimieren

Gemäss Schritten 1 und 2 und Ihren positiven Antworten wurden also die organisatorischen Vorkehrungen und technischen Anpassungen gemacht. Nun gilt es wie die Feuerwehr für den Fall einer Ransomware Attacke oder Hacker Angriffs bereit zu sein. Was muss wie gemacht werden, um den Schaden zu minimieren?

Ende 2016 erfolgte alle 40 Sekunden eine Ransomware Attacke oder Angriff. Alle 14 Sekunden passierte dies 2019 und alle 11 Sekunden in 2021.

DrKPI® und andere Experten wie z.B. Sophos schätzen, dass **diese Zahl auf 7 - 9 Sekunden Ende 2022 sinken wird**.

Rund 960 - 1200 Attacken **pro Tag** werden in der Schweiz registriert. Die Dunkelziffer kann niemand wirklich abschätzen.

Firmen mit mehr als 249 Vollzeit Angestellten, d.h. nicht KMU, haben eine 70% Chance, dass sie in den **nächsten 18 Monaten Opfer einer "erfolgreichen" Ransomware oder Hacker Attacke** sein werden.

Können Sie die folgenden Fragen mit **JA** beantworten?

1. Überwacht Ihr Unternehmen steuerungsrelevante KPIs für Cybersecurity?

Was sind die möglichen Schwachstellen und Lücken bei den Cybersicherheit-Control Mechanismen?

Beschränken Sie sich auf 2 bis 4 wirklich relevante Kennzahlen. Wie schnell kann/muss eine durch das Bug-Bounty bekannt gemachte Vulnerability nach deren Triage und Gefahreneinstufung gepatcht werden?

Ohne die Dinge zu messen ist es schwierig, diese zu steuern und zu managen.

2. Ist Ihr Unternehmen auf eine Reaktion und Wiederherstellung vorbereitet?

Tests: Validierte Backups mit getesteter Wiederherstellung der Infrastruktur (z. B. Active Directory) mind. 2 x im Jahr. Solche Übungen können am Wochenende geschehen, um die reguläre Arbeit nur geringfügig zu stören.

Backups müssen an verschiedenen Orten aufbewahrt werden. Das heisst, weder in der Cloud von Microsoft (Achtung U.S. Cloud Act) noch auf dem Betriebsgelände oder beim IT-Dienstleister. Wichtig ist die Regel: " Possession is nine-tenths of the law."

Wichtig ist zu testen, wie schnell und mit welchem Arbeitsaufwand mit Hilfe dieser Backups Daten für wichtige Applikationen zu 100% wiederhergestellt werden können.

3. Kontrolliert Ihr Unternehmen regelmässig den Umsetzungsstatus der Cybersecurity Strategie?

Nur dank der Überprüfung wissen Sie, ob das gesetzte Ziel erreicht werden kann. Beispielsweise, funktionieren die Notstromaggregate beim Cloud Provider, im Haus oder anderswo? Diese Dinge müssen regelmässig in Tests überprüft werden.

4. Ist das Unternehmen auf die Krisenkommunikation vorbereitet?

Wenn die Ransomware Attacke stattfand, muss darüber transparent innert 12 Std. kommuniziert werden. Der Firmenblog mit eingebauten Screenshots ist das ideale Instrument. Template vorbereiten spart Zeit im Notfall und schont Ihre Nerven.

Schlagwörter und Kennzahlen im Auge zu behalten, ist der Schlüssel zum Erfolg. Die gesamte Thematik der Cybersecurity und VDP / Bug-Bounty Management ist ein fortlaufender Prozess: System Owners und Nutzer:innen dürfen nie nachlassen und müssen sich die Best Practice Regeln und das iSLA stets vor Augen führen.

Programmierer müssen auf dem neusten Stand bleiben, denn die Technologie entwickelt sich pausenlos weiter. Es ist nicht leicht, mit den neuesten Trends Schritt zu halten. Gehen Sie davon aus, dass die Hacker das tun.

Bei Fragen zur Umsetzung unserer Tipps für effektive Vulnerability Disclosure und Cybersecurity Prozesse helfen wir Ihnen gerne weiter. Rufen Sie einfach an oder schreiben Sie uns eine Mail. Unsere Kontaktdaten finden Sie unten. Wir freuen uns auf Sie.

Ressourcen

Hier finden Sie weitere Informationen zu diesem SchnellAudit inkl. Blogeinträge zum Thema, Ratgeber und Checklisten zum Download (ANKLICKEN):

- ☐ 8 Schritte zum erfolgreichen Vulnerability Disclosure Programm
- ☐ Sicherheitslücken schliessen dank Vulnerability Disclosure Programm (Complete Guide)
- ☐ Responsible Disclosure Programm: Leitfaden und Tipps für Ihre Datensicherheit
- ☐ Vulnerability Disclosure Programm: Welche Prozesse helfen (Juni 2022)

Über DrKPI®

DrKPI® Cybersecurity ist eine Division der CyTRAP Labs GmbH. Sie unterstützt Unternehmen dabei, eine erfolgreiche Cybersecurity Strategie zu entwickeln. Wir bieten unseren Kunden know-how in den Bereichen Sicherstellung der DSGVO-Compliance bis zur Erstellung von Vulnerability Disclosure Programmen und Prozessen.

Der DrKPI® PageTracker ist unsere einzigartige Software für die Webseitenoptimierung, mit der Sie den Erfolg Ihrer Corporate Communication messen und sich gezielt mit Konkurrenten in Ihrer Branche vergleichen können. Website optimieren, Marke stärken und beim Reporting überzeugen.

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