Beispielanwendung

Continual-Improvement (CI) Modell

Sebastian Meisel

13. März 2023

1 Szenario

Eine SWOT-Analyse hat Ransomware-Angriffe als akutes Risiko identifiziert und Schwächen in der Abwehr solcher Angriffe erkannt. Nun sollen Maßnahmen ergriffen werde, um die Bedrohung zu minimieren.

1.1 Was ist unsere Vision?

Unsere Unternehmen soll innerhalb des nächsten Jahres ein umfassendes Konzept zur Disaster-Recovery[1] bei einem erfolgreichen Ransomware-Angriff, sowie ein geeignetes Konzept zur Prävention eines solchen Angriffes erarbeiten.

1.2 Wo stehen wir?

Zunächst muss die Ist-Situation ermittelt werden. Dies beinhaltet die Identifizierung der **Assets**[2], die am anfälligsten für Angriffe sind. Dazu muss ein umfassender **Vulnerabilty-Scan** erfolgen sowie die **Überprüfung der Sicherheitsprotokolle** und z.B. der **Firewall**-Implementierung. Schließlich muss die aktuelle **Backupstrategie** dokumentiert werden. Auch die Kompetenz der IT-Abteilung in Bezug auf auf Strategien zur Abwehr von Ransomware-Angriffen muss überprüft werden.

1.3 Wo wollen wir hin?

In diesem Schritt sollen konkrete Ziele (S.M.A.R.T.) formuliert, Metriken (KPIs) zur Messung der Zielerreichung und Maßnahmen zum erreichen dieser Ziele erarbeitet werden. Dabei kann eine Gap-Analyse helfen.

[1] Maßnahmen zur Wiederherstellung eines funktionsfähigen Betriebs nach einem Ereignis, dass den Fortbestand des Unternehmens gefährden oder seinen Marktwert signifikant senken kann.
[2] Software und Hardwarekomponenten, die einen finanziellen Wert für das Unternehmen darstellen.

1.3.1 Key Performance Indikators (KPIs)

KPIs sind Metriken (Messwerte), die in Bezug auf eine konkrete Fragestellung besonders aussagekräftig sind. Ziel ist es wenige KPIs zu wählen anhand derer weitere Entscheidungen getroffen werden und die gleichzeitig bei der Bewertung des Erfolgs von Verbesserungsmaßnahmen helfen.
Es gibt eine Vielzahl von KPIs, die bei der Bewertung der IT-Sicherheit in Bezug auf die Sicherheit einer Backupstrategie verwendet werden können. Die Auswahl der KPIs hängt von den Anforderungen des Unternehmens ab und sollte in Zusammenarbeit mit den relevanten Stakeholdern identifiziert und priorisiert werden.

Backup-Zeitfenster: Die Zeit, die benötigt wird, um eine vollständige Sicherung aller relevanten Daten abzuschließen. Ein kürzeres Backup-Zeitfenster kann darauf hindeuten, dass die Backupstrategie optimiert und die Backup-Infrastruktur gut konfiguriert ist.

Recovery Point Objective (RPO): Die maximale Datenmenge, die im Falle eines Ausfalls oder einer Störung verloren gehen kann. Ein niedriger RPO zeigt an, dass die Backupstrategie effektiv ist und es wenig Datenverlust im Falle eines Ausfalls geben wird.

Recovery Time Objective (RTO): Die maximale Zeit, die benötigt wird, um die Geschäftsprozesse nach einem Ausfall wiederherzustellen. Ein niedriger RTO zeigt an, dass die Backup- und Wiederherstellungsfunktionen effektiv sind.

Anzahl der erfolgreichen Wiederherstellungen: Die Anzahl der Wiederherstellungen, die erfolgreich durchgeführt wurden. Eine hohe Anzahl erfolgreicher Wiederherstellungen zeigt an, dass die Backupstrategie effektiv ist.

Anzahl der Backup-Fehler: Die Anzahl der Fehler, die bei der Durchführung von Backups aufgetreten sind. Ein niedriger Wert zeigt an, dass die Backupstrategie stabil ist und dass das Backup-System gut funktioniert.

Daten-Integrität: Ein Indikator dafür, ob die Sicherungskopien der Daten tatsächlich wiederhergestellt werden können und die Integrität der Daten gewährleistet ist. Ein geringer Wert deutet darauf hin, dass die Backupstrategie überarbeitet werden muss.

Kosten für Backup und Wiederherstellung: Die Kosten für die Implementierung und Wartung von Backup- und Wiederherstellungslösungen. Eine Senkung der Kosten könnte darauf hindeuten, dass die Backupstrategie effektiv ist und optimiert wurde.

1.3.2 Gap Analysis

Eine Gap-Analyse in Bezug auf eine Backupstrategie kann dazu beitragen, potenzielle Lücken oder Schwachstellen in der aktuellen Backupstrategie zu identifizieren. Eine solche Analyse könnte wie folgt aussehen:

Anforderungsanalyse: Zunächst sollten die Anforderungen an die Backupstrategie festgelegt werden. Dazu gehören RPO, RTO, Datenintegrität und Backupzeitfenster.

Ist-Analyse: In diesem Schritt wird die aktuelle Backupstrategie bewertet. Hier werden die vorhandenen Backup-Lösungen, -Prozesse und -Technologien untersucht. Es sollten Fragen gestellt werden, wie zum Beispiel:

- Welche Backup-Methoden und Technologien werden derzeit eingesetzt?
- Welche Daten werden gesichert und wie häufig?
- Wie oft werden die Backup-Systeme getestet?
- Wie lange dauert es, um die Daten wiederherzustellen?
- Wie wird die Sicherheit der Backup-Daten gewährleistet?
- Wie gut sind die Backup- und Wiederherstellungsprozesse dokumentiert?

Soll-Analyse: In diesem Schritt wird der gewünschte Zustand der Backupstrategie definiert, basierend auf den Anforderungen und der Ist-Analyse. Die Soll-Analyse sollte klare Ziele und Maßnahmen zur Verbesserung der Backupstrategie enthalten.

Identifikation von Lücken: In diesem Schritt wird der Unterschied zwischen dem aktuellen Zustand (Ist-Analyse) und dem gewünschten Zustand (Soll-Analyse) analysiert, um Lücken und Schwachstellen zu identifizieren.

Priorisierung von Maßnahmen: Basierend auf den identifizierten Lücken und Schwachstellen sollten Prioritäten für die Umsetzung von Maßnahmen festgelegt werden. Die Maßnahmen können beispielsweise die Einführung neuer Backup-Methoden, die Verbesserung der Backup-Technologien oder die Schulung von Mitarbeitern umfassen.

Umsetzung und Überwachung: Nach der Festlegung von Maßnahmen sollte ein Plan für deren Umsetzung erstellt werden. Die Umsetzung sollte sorgfältig überwacht und die KPIs regelmäßig bewertet werden, um sicherzustellen, dass die Ziele erreicht werden.

1.4 Es angehen!

Das IT-Team setzt den Plan um, um die Sicherheitsmaßnahmen zu stärken. Dies kann die Aktualisierung von Software-Patches, die Überprüfung der Sicherheitsprotokolle und die Stärkung der Firewall umfassen.
Das IT-Team überwacht und misst regelmäßig die Effektivität der neuen Sicherheitsmaßnahmen. Dazu werden die zuvor festgelegten KPIs gemessen, um den Fortschritt der Verbesserungen zu verfolgen.

1.5 Sind wir dahin gekommen?

Das IT-Team bewertet regelmäßig die KPIs und identifiziert Verbesserungsmöglichkeiten, um die Effektivität der Sicherheitsmaßnahmen weiter zu steigern. Zum Beispiel könnten Schulungen für Mitarbeiter durchgeführt werden, um sie für die Risiken von Ransomware-Angriffen zu sensibilisieren oder die Implementierung neuer Technologien zur Verbesserung der Cyber-Sicherheit in Betracht gezogen werden.

1.6 Wir bleiben wir dran?

Erfolge in der Abwehr von pontentiellen Angriffen, sollten kommuniziert werden. Zugleich gilt es neue Angriffswege im Blick zu behalten und die Abwehrstrategien stätig anzupassen.

1.6.1 Mitarbeiter begleiten

Die Stärkung von IT-Sicherheitskonzepten kann für Mitarbeitende auch mit einigen Belastungen verbunden sein. Es ist wichtig zu betonen, dass die Stärkung von IT-Sicherheitskonzepten auch Vorteile für die Mitarbeitenden haben kann, z.B. durch eine erhöhte Sicherheit ihrer Daten und eine verbesserte Compliance mit relevanten Vorschriften.
Es ist daher ratsam, die Belastungen und Vorteile sorgfältig abzuwägen und sicherzustellen, dass die Mitarbeitenden angemessen geschult und informiert werden, um mögliche negative Auswirkungen auf ein Minimum zu reduzieren, um die Bereitschaft solche Verbesserungen anzugehen zu erhalten.
Hier sind einige der Möglichen Belastungen zusammengestellt:

Einschränkungen bei der Nutzung von IT-Ressourcen: Die Stärkung von IT-Sicherheitskonzepten kann bedeuten, dass Mitarbeitende in ihrer Nutzung von IT-Ressourcen eingeschränkt werden, z.B. durch den Einsatz von Zugangskontrollen, Firewall-Regeln oder Passwortrichtlinien. Dies kann als störend empfunden werden und den Workflow beeinträchtigen.

Zusätzliche Schulungen und Trainings: Um sicherzustellen, dass Mitarbeitende die neuen IT-Sicherheitskonzepte verstehen und anwenden können, müssen sie möglicherweise zusätzliche Schulungen und Trainings absolvieren. Dies kann zusätzlichen Zeitaufwand bedeuten und unter Umständen als Belastung empfunden werden.

Höherer Zeitdruck: Die Stärkung von IT-Sicherheitskonzepten kann zu einem höheren Zeitdruck führen, insbesondere wenn Mitarbeitende zusätzliche Überprüfungen oder Maßnahmen durchführen müssen, um sicherzustellen, dass die Sicherheitsstandards eingehalten werden. Dies kann zu einem erhöhten Stressniveau und einer Belastung der Arbeit führen.

Veränderungen im Arbeitsumfeld: Wenn sich IT-Sicherheitskonzepte ändern, kann dies Veränderungen im Arbeitsumfeld mit sich bringen, z.B. durch die Einführung neuer Technologien oder die Umstellung auf neue Prozesse. Dies kann eine Einarbeitungsphase erfordern und zu Unsicherheiten und Unwohlsein bei den Mitarbeitenden führen.