Sicherheitsprozesse gegen Cyber-Attacken etablieren

Die Frage ist nicht ob, sondern wann ...

... ein Hacker-Angriff erfolgt. Vermeiden lassen sich derartige Attacken nicht, aber es gibt eine Reihe von Maßnahmen, mit welchen sich Unternehmen und Anwender:innen vorbereiten können. Die Sprecher des DSAG-Arbeitskreises Security & Vulnerability Management sowie der Arbeitsgruppen Cloud Security und Identity Management (IdM) 8.x geben Tipps, wie man sich gegen Cyber-Angriffe wappnen kann.

Thomas Kircher, blaupause-Redaktion

Treffen kann es jede:n. Sei es der Stahlgroßhändler, der Automobilzulieferer, das Kosmetik- und Chemieunternehmen oder die Mediengruppe. Das Problem: Einem Hacker-Angriff vorzubeugen, ist schlicht unmöglich. Die Frage ist lediglich, wann ein Angriff erfolgt oder ob er nicht vielleicht schon stattgefunden hat. Denn die Attacken passieren nicht von jetzt auf gleich. „Der durchschnittliche Zeitraum, in dem ein Vorfall entdeckt wird, beträgt aktuell ca. 200 Tage und eine vollständige Bereinigung etwa 270 Tage", weiß Andreas Kirchebner, Sprecher der DSAG-Arbeitsgruppe Cloud Security, und bezieht sich damit auf Angaben aus dem IBM Cost of a Data Breach Report 2022. Das heißt, Angreifer:innen können rund ein dreiviertel Jahr in einem System befinden, Daten abziehen, Programme manipulieren oder gar stilllegen – und noch viel wichtiger und gefährlicher: ihre Spuren verwischen.

Schwachstellen nehmen zu

Auch wenn sich derartige Angriffe nicht vermeiden lassen, kann immerhin die Angriffsfläche verkleinert werden. Damit sind wir beim Stichwort „Bewusstsein schaffen" (Awareness) und auch gleich beim Schwachpunkt: dem Menschen. Denn Mitarbeiter:innen sind und waren in der Vergangenheit eines der Haupteinfalltore für Cyber-Angriffe per so genannter Social-Engineering-Attacken wie z. B. Phishing-Kampagnen. Durch die zunehmende Vernetzung, die steigende Zahl an IT-Lösungen und exponierten Services wie Cloud-Lösungen nehmen aber auch die Schwachstellen in den IT-Lösungen selbst zu. „Diese Einfallsvektoren sind schwer zu harmonisieren und zu kontrollieren und darum offene Flanken, über die auf sensible Daten zugegriffen werden kann", weiß Axel Daldorf, stellvertretender Sprecher des Arbeitskreises Security & Vulnerability Management.

Cyber-Security-Ökosystem – welche Schritte wichtig sind:

- Was ist zu schützen?
- Welche Prozesse sind wichtig?
- Was ist darüber hinaus noch zu tun?
- Was ist das Ziel?
- Gibt es Lösungen und einen Fahrplan dahin?
- Ist Logging aktiviert?
- Welche Maßnahmen sind umzusetzen?
- Welche Prozesse sind zu etablieren, zu überwachen oder zu optimieren?
- Welche Ziele sind an geänderte Geschäftsprozesse anzupassen?

Angriffsziele verändern sich

Auf SAP bezogen lässt sich feststellen, dass in den vergangenen drei bis vier Jahren auch Enterprise-Resource-Planning (ERP)-Systeme verstärkt in den Fokus von Attacken geraten sind. „SAP versucht seine Programme so gut wie möglich mit Sicherheitshinweisen abzusichern. Damit diese greifen können, sind die Unternehmen allerdings in der Bringschuld, indem sie entsprechende Updates und Patches zeitnah einspielen", erläutert Oliver Villwock, stellvertretender Sprecher der Arbeitsgruppe Cloud Security.

v. l. n. r.: Axel Daldorf, stellvertretender Sprecher des Arbeitskreises Security & Vulnerability Management, Andreas Kirchebner, Sprecher der DSAG-Arbeitsgruppe Cloud Security, Aydin Tekin, Sprecher der Arbeitsgruppe IdM 8.x, Oliver Villwock, stellvertretender Sprecher der Arbeitsgruppe Cloud Security, und Alexander Ziesemer, Sprecher des Arbeitskreises Security & Vulnerability Management

Darüber hinaus sollten ein eigener Incident-Response-Prozess und mögliche Playbooks aufgesetzt werden. „Um sich auf einen Angriff vorzubereiten, braucht es exakte Abläufe, die festlegen, was zu tun ist, wenn er erfolgt. Welche Schritte greifen sollen. Wer in welchem Fall wie eingebunden werden muss. In bestehende Landschaften, die seit vielen Jahren laufen, ist ein derartiger Prozess aber nicht so einfach zu integrieren", erläutert Alexander Ziesemer, Sprecher des Arbeitskreises Security und Vulnerability Management. Es kann auch helfen, so genannte Business-Continuity-Management (BCM)- oder auch IT-Service-Continuity-Management (IT-SCM)-Pläne aufzusetzen (siehe Glossar Seite 22), und zwar nicht nur auf Infrastruktur-, sondern auch auf Applikationsebene.

Kein „One Size fits all" möglich

Aber auch „Cyber-War-Games" können eine gute Maßnahme sein. Das heißt, einen möglichen Angriff zu üben. Beispielsweise einen Recovery-Prozess starten und sehen, was dabei herauskommt, kann eine gute Übung sein, aus der man im Idealfall wichtige Erkenntnisse zieht. „Die Feuerwehr übt ja auch regelmäßig, um bestens vorbereitet zu sein", fasst Axel Daldorf zusammen. Wie immer die Maßnahmen dann auch aussehen mögen, sicher ist, es gibt kein „One Size fits all". Das Bedrohungsszenario ist in jedem betroffenen Unternehmen anders.

Hausaufgaben erledigen

Ziel muss es sein, einen Angriff oder Angriffsversuch in einem frühen Cyber-Kill-Chain-Level (siehe Glossar Seite 22) zu erkennen, um noch zum Zeitpunkt des geringsten Schadens reagieren zu können. Da geht es dann um Sys- →

temhärtung und eine entsprechende Überwachung. „In weiterer Folge stehen Risk-Management, Assets und Impact-Analysen, also die tatsächlichen Auswirkungen, auf der Agenda", so Andreas Kirchebner. Schlagworte wie „Zero Trust" und „Assume Breach" tauchen in diesem Kontext auf – oder anders formuliert: Traue niemandem und gehe immer von einem Angriff aus. „Genauso müssen wir uns heute aufstellen und Systeme aufbauen. Das muss das Mindset sein", weiß Andreas Kirchebner. Und dafür sind Hausaufgaben zu erledigen, z. B. in Form eines resilienten Cyber-Security-Ökosystems (siehe Kasten Seite 20).

Schnittstelle zu Kund:innen ist ausbaufähig

Was Cloud-Lösungen betrifft, ist SAP selbst gut geschützt. Die Schnittstellen zu den Kund:innen hingegen sind noch ausbaufähig. Die schnelle und zielführende Kommunikation von SAP mit Anwender:innen, wenn etwas geändert oder eine Schwachstelle festgestellt wird, birgt aber noch Verbesserungspotenzial. „Inhaltlich und technisch sollte SAP dazu in der Lage sein, aber Transparenz und Kommunikation sind hier noch nicht ausgereift genug. Wenn SAP hierfür mehr Zeit und Ressourcen investieren würde, könnte das wesentlich zu einem besseren Gefühl bei den Kundenunternehmen beitragen", ist Aydin Tekin, Sprecher der Arbeitsgruppe IdM 8.x, überzeugt. Dennoch lohnt ein Blick in den SAP EarlyWatch Alert (siehe Glossar Seite 22), um schnell einen Überblick über die SAP-Herstellerempfehlungen zu möglicherweise kritischen Situationen zu erhalten.

Netzwerken ist das A und O

Information und Unterstützung liefern auch die DSAG-Gremien, die sich mit dem Thema Security auseinandersetzen. Der Erfahrungsaustausch über organisatorische und technische Maßnahmen sowie das Netzwerken unter den Mitgliedspersonen sind dabei das A und O. Awareness ist aktuell ein sehr wichtiges Thema im Arbeitskreis Security & Vulnerability Management, wie auch der Umgang mit den Tools von SAP, das SAP Security Baseline Template und natürlich die Cloud-Security-Empfehlungen (siehe Info-Icon). „Je mehr IT-Dienste nur noch in der Cloud verfügbar sind, desto mehr müssen die ERP-On-Premise-Sicherheitskonzepte auf den Prüfstand gestellt werden. Ein SAP-Security-Best-Practice-Leitfaden wäre da z. B. eine wichtige Sache, und genau damit will sich der Arbeitskreis in Zukunft beschäftigen", fasst Alexander Ziesemer zusammen. In puncto Sicherheit ist also immer etwas zu tun, das ist sicher! ■

Cloud-Security-Empfehlungen
support.sap.com/sos
sap.com/documents/2022/12/7616adbb-547e-0010-bca6-c68f7e60039b.html

Glossar

Cyber-Kill-Chain
Die Cyber-Kill-Chain wurde von Lockheed Martin entwickelt, um Cyber-Angriffe zu beschreiben. Sie besteht aus mehreren Stufen, die ein immer tieferes Vordringen der der Angreifenden beschreiben.
Phase 1: Erkundung
Phase 2: Passende Angriffsmethode finden
Phase 3: Gezielter Angriff
Phase 4: Brückenkopf
Phase 5: Übernahme
(Quelle: wikipedia.org)

Ransomware
Der Begriff Ransomware steht für eine Art von Schadprogrammen, die den Zugriff auf Daten und Systeme einschränken oder unterbinden. Für die Freigabe wird dann ein Lösegeld (englisch: Ransom) verlangt. Entweder sperrt ein solches Schadprogramm den kompletten Zugriff auf das System, oder es verschlüsselt bestimmte Nutzerdaten. Besonders verbreitet ist Ransomware, die sich gegen Windows-Rechner richtet. Prinzipiell aber können alle Systeme von Ransomware befallen werden. *(Quelle: BSI)*

Business-Continuity-Plan
Ein Business-Continuity-Plan (BCP) umfasst eine detaillierte Strategie und eine Reihe von Systemen, mit denen ein Unternehmen erhebliche Unterbrechungen des Betriebsablaufs verhindern oder notfalls eine schnelle Wiederherstellung durchführen kann.

SAP Security Baseline Template
Die Vorlage für die Sicherheitsgrundlagen enthält ein umfangreiches 80-seitiges Word-Dokument, das alle Themen der SAP Secure Operations Map abdeckt.

support.sap.com/content/dam/support/en_us/library/ssp/offerings-and-programs/support-services/sap-security-optimization-services-portfolio/Security_Baseline_Template_V2.zip

SAP-Security
SAP bietet ein umfassendes Portfolio an Sicherheitsprodukten und -Services, mit denen sich Daten und Unternehmen schützen lassen.

community.sap.com/topics/security

SAP EarlyWatch Alert
SAP EarlyWatch Alert ist ein automatischer Dienst, der die wesentlichen Verwaltungsbereiche eines SAP-Systems analysiert. Alerts weisen auf kritische Situationen hin und bieten Lösungen zur Verbesserung von Performance und Stabilität. Um diese Alerts zu prüfen und anzuzeigen, bietet SAP den SAP EarlyWatch Alert Workspace an, wo auch die vollständigen Ergebnisse als Berichtsdokument heruntergeladen werden können.

support.sap.com/en/offerings-programs/support-services/earlywatch-alert.html