Von der klassischen Schutzorientierung zur proaktiven Cleverness

«Assume the breach» ist das neue Zauberwort im Cybersecurity-Bereich. Also nicht ob, sondern wann ein Unternehmen durch Kriminelle angegriffen wird (oder schon wurde). Es gilt, den Angreifern möglichst früh den Wind aus den Segeln zu nehmen. Höchste Zeit also, dem CISO einen «Seat at the Table» zu offerieren und sich auf Angriffe vorzubereiten.

Die Autorin
Monika Josi, Head IT Consulting, Avectris

Neu eingeführte Technologien oder Modelle wie Cloud, künstliche Intelligenz, Big Data, Internet der Dinge oder DevOps und agile Projektmethoden treffen heute auf historisch gewachsene IT-Infrastrukturen, statische Sicherheitsmodelle-/standards und altbewährte Prozesse. Das Cybercrime-Umfeld hat sich in den letzten Jahren stark professionalisiert. Die Angriffe erfolgen heute nicht mehr klassisch übers Netzwerk, sondern auf immer heimtückischere Art über die schwächsten Glieder im Unternehmen – wie etwa längst bekannte Schwachstellen, die Lieferkette oder über Phishing-Attacken. Wenn bewährte Schutzmauern allein nicht mehr reichen und die Prävention der Realität immer einen Schritt hinterherhinkt, muss ein Umdenken stattfinden.

Chief Information Security Officer (CISOs) stehen vor der herausfordernden Aufgabe, ihr Unternehmen von einer compliance-basierten zu einer agilen Sicherheitsorganisation zu wandeln. Es gilt, sich auf bisher unbekannte Risiken in einem sich dauernd ändernden IT-Umfeld rasch einzustellen, um entsprechend reagieren zu können.

Ganzheitlich identifizieren, aufdecken und sofort reagieren

Das anerkannte «NIST Cyber Security Framework» beinhaltet Sicherheitsempfehlungen für kritische Infrastrukturen und lässt sich bei mittelständischen Unternehmen effizient umsetzen. Kern der Empfehlungen bilden die Punkte «identifizieren, absichern, aufdecken, reagieren und wiederherstellen», die den gesamten Informationssicherheitszyklus abdecken. Um den Wandel von einer rein schutzorientierten Ausrichtung zum detektions- und reaktionsbasierten Ansatz zu vollziehen, muss eine risikobasierte und agile Strategie zur Stärkung der Cyber-Resilienz gewählt werden. Dabei analysiert der Berater die Umgebung, die Bedrohungslage und wählt schliesslich die passende Strategie. Auch Compliance- und Risikomanagement-Aspekte müssen in der richtigen Balance adressiert werden.

Aus Technologiesicht sollten folgende mögliche Schwachstellen, respektive Angriffsziele berücksichtigt werden:

- unterschiedliche Eintrittspunkte (Notebooks, Mobiltelefone und Server)
- Identity- und Access-Management-Systeme inklusive Privileged Access Management
- Core-Infrastruktur
- Entwicklungsprozess (inkl. DevOps) sowie die verwendeten Applikationen

Auch die eingesetzten Sicherheitstechnologien gilt es zu prüfen. Diese sind oft historisch gewachsen, entsprechen häufig nicht den aktuellen Anforderungen oder decken nicht alle relevanten Aspekte ab. Die Sicherheit Ihres Unternehmens ist kein definiertes Endprodukt von der Stange. Letztlich gilt: Die Umweltanalyse und aktuelle Bedrohungslage sind regelmässig neu zu beurteilen und passende Reaktionsszenarien einzuleiten.

Umgebungsanalyse	Bedrohungslange	Strategie
Identifikation der Umgebung und der Risiken/Schwachstellen aus Geschäftssicht (kritische Assets, Prozesse, Lieferkette) und Technologiesicht (inkl. Berücksichtigung der Schatten-IT inkl. SaaS) und der relevanten Compliance-Anforderungen (z.B. Datenschutz, Finma, GxP)	Identifikation der wahrscheinlichsten Angriffsszenarien, Vorgehensweisen und Angriffsziele. Ausser Ransomeware-Attacken sind auch Social Engineering und Phishing-Attacken zu berücksichtigen.	Priorisierte Strategie nach dem NIST-Modell mit Soll-/Ist-Abgleich. In einer ersten Phase liegt die Priorität bei den als kritisch eingestuften Aktivitäten. Dabei sind die Aspekte «People – Process – Technology» zu berücksichtigen und aufeinander abzustimmen.

«Es muss vorab geklärt werden, welche Prozesse prioritär sind»

Es genügt nicht, ein wachsames Auge zu haben. Wer wirklich sicher sein will, muss viel mehr im Blick haben als die potenziellen Bedrohungen durch Cyberattacken. Was sonst noch dazugehört, sagt Monika Josi, Head IT Consulting bei Avectris. Interview: Coen Kaat

Wie sieht der optimale Schutz für Unternehmen aus?
Monika Josi: Ransomware-Attacken haben deutlich gemacht, dass drei Aspekte zum bestmöglichen Schutz zentral sind: Die rasche Behebung von Schwachstellen, beispielsweise durch Patching, das automatisierte Erkennen von verdächtigem Verhalten durch ein Security Operation Center (SOC) sowie die zeitnahe (automatisierte) Reaktion auf kritische Aktivitäten. Business-Continuity-Aspekte spielen ebenfalls eine wichtige Rolle.

Inwiefern?
Es muss etwa vorab geklärt werden, welche Geschäftsprozesse prioritär sind, wenn die Core-IT innerhalb von wenigen Stunden total ausfällt und die Wiederherstellung Tage oder Wochen dauern könnte. Die einzelnen NIST-Komponenten betrachtet der erfahrene CISO dabei nicht isoliert, sondern berücksichtigt deren Wechselwirkung aufeinander.

Sind nicht alle geschäftskritischen Prozesse prioritär? Wie definiert ein Unternehmen die wichtigen Prozesse?
Meist über monetäre Werte. Dies können zum Beispiel alle Prozesse sein, welche die Herstellung und den Verkauf eines Produkts sicherstellen, das den Grossteil des Umsatzes ausmacht. Bei Dienstleistungsunternehmen ist es ähnlich. Hier ist die Frage, welche Dienstleistung am meisten Geld bringt und damit das Überleben der Firma sichert. Dies können auch «Supportprozesse» wie beispielsweise das finanzielle Reporting betreffen.

Was ist der nächste Schritt, wenn die prioritären Prozesse definiert sind?
Darauf basierend eruieren wir die Abhängigkeiten von den unterstützenden Prozessen einerseits und der Core-IT andererseits. Kritisch ist insbesondere die Sicherung der Verzeichnisdienste wie etwa Active Directory, die so etwas wie das Telefonbuch für das Unternehmen darstellt.

Reicht es, ein wachsames Auge zu haben, um sicher zu sein?
Nein. Fakt ist, dass fehlende Sicherheitsmassnahmen im präventiven Bereich nicht durch detektive Massnahmen, wie beispielsweise Monitoring im SOC, wettgemacht werden können, sondern es muss immer der ganze NIST-Zyklus berücksichtigt werden.

Worauf gilt es dabei zu achten?
Die Umweltanalyse und aktuelle Bedrohungslage sind regelmässig neu zu beurteilen und passende Reaktionsszenarien einzuleiten.

Monika Josi, Head IT Consulting, Avectris.

VERANSTALTUNG

Am «Avectris Day», der am 21. Mai im Trafo in Baden stattfindet, gibt es 13 Fachvorträge, 3 davon zum Thema Cybersecurity. Hier erfahren Besucher mehr zur aktuellen Bedrohungslage, Umsetzungsstrategien, Bereitschaft dank Cyber-BCM-Szenarien und der digitalen Ermittlungszentrale Security Operations Center.

Kostenlose Anmeldung:
www.avectris.ch/AD19