Status xy ungelöst

Von Schwierigkeiten und Lösungsansätzen zur Messbarkeit von Sicherheit am Beispiel von Resilienz gegenüber Ransomware

Die Messbarkeit von Cyber-Sicherheit und die Qualität solcher Messungen ist noch immer an vielen Stellen ein Problem. Unsere Autoren möchten den Diskurs hierzu befeuern, sich dem Thema strukturiert nähern und zum gemeinsamen Weiterdenken und Bessermachen einladen.

Von Florian Oelmaier, Falko Weiß und Arthur Naefe, München

Wir arbeiten in der IT – wir alle haben eine technische Ausbildung, viele von uns haben wissenschaftliches Arbeiten an der Universität gelernt. Wir lieben Entscheidungen, die sich auf Zahlen, Daten und Fakten stützen. Dennoch können wir auf einfache Fragen des Managements – „Wie sicher sind wir vor Cyberangriffen? Wie gut ist unser Unternehmen gegen Ransomware geschützt?" – oft keine leicht verständliche und vor allem messbar nachvollziehbare Antwort liefern. Üblicherweise erläutern wir dann, was wir in den letzten Monaten alles zur Absicherung getan haben oder verweisen auf Prüfungen nach aktuellen Standards. Aber ist unser Bild vollständig? Nach welcher Methodik messen wir Erfolge? Haben wir überhaupt etwas „gemessen" oder doch eher nur „abgeschätzt"?

Was wollen wir messen?

Diverse Qualitätsmodelle (z. B. Donabedian) unterscheiden zwischen Struktur-, Prozess- und Ergebnis-Qualität. Dabei beeinflussen die Strukturqualität (Fähigkeit der Mitarbeiter, Qualität der Maschinen usw.) und die Prozessqualität (Reife) das Wichtigste: die Ergebnisqualität (wie gut sind Produkte/Dienstleistungen oder eben auch das tatsächliche Sicherheitsniveau?). Angewendet auf die IT-Sicherheit lassen sich die drei Dimensionen wie folgt unterscheiden:

– *Strukturelle Sicherheit:* Hierunter kann man personelle Ressourcen der Sicherheitsabteilungen, die Sicherheits-Awareness von Mitarbeitern und Führungspersonal, die Investitionsbereitschaft des Managements in Sicherheitsthemen sowie Quantität und Qualität der vorhandenen Sicherheitstools verstehen – inklusive dem Know-how der Mitarbeiter, um diese sinnvoll einzusetzen. Die strukturelle Sicherheit eines Unternehmens baut sich erst langfristig auf und ist kurzfristig kaum beeinflussbar. Strukturqualität ist schwer messbar, weswegen Manager sie bisweilen gering schätzen.

– *Prozessreife in der Sicherheit:* Zu den Sicherheitsprozessen gehören zum Beispiel ein qualitativ hochwertiges und dokumentiertes Informationssicherheits-Managementsystem (ISMS) sowie ein Prozess zur Ermittlung und Beurteilung von Informationssicherheits-Risiken. Auch operative Prozesse zur Behandlung von Sicherheitsvorfällen und Managementprozesse, wie die Sicherheitsstrategie und das zugehörige Change-Programm, fallen in diese Kategorie. Die Existenz von Sicherheitsprozessen ist wohl am leichtesten messbar. Zudem lassen sich Prozesse vergleichsweise einfach abstrahieren und kategorisieren. Das hat den Vorteil, dass Änderungen an den Prozessvorgaben weniger häufig notwendig werden. Viele der gängigen IT-Standards (z. B. ISO 27001, ITIL und TISAX) fokussieren daher stark auf die Prozesse.

– *Realisierte Sicherheit:* Jede IT-Landschaft steht einer – firmenspezifisch oft unterschiedlichen – Reihe von Bedrohungen gegenüber. Am Ende stehen die Fragen: Wie resilient ist eine Unternehmens-IT gegen diese Bedrohungen? Wie gut kann man die Eintrittswahrscheinlichkeit reduzieren und Schäden minimieren? Das ist das „Ergebnis", das am Ende zählt! Die Ergebnisqualität kann man jedoch nicht direkt erhöhen: Verbesserungen erfordern immer Optimierungen der strukturellen Sicherheit und/oder den Sicherheitsprozessen.

Aktuelle Mess-Ansätze

Um die Qualität der Sicherheit zu messen, benötigt man gute Messinstrumente. Aber welche Qualitätskriterien sind an diese Messinstrumente zu stellen? In der Wissenschafts-Ethik werden zwölf zentrale Qualitätskriterien angewendet, um wissenschaftliche Arbeit zu bewerten [1]: Ehrlichkeit, *Objektivität, Überprüfbarkeit, Reliabilität (Wiederholbarkeit), Validität (Genauigkeit), Verständlichkeit, Relevanz,* logische Argumentation, Originalität, *Nach-*

vollziehbarkeit, Fairness und Verantwortung. Gerade die in der Aufzählung kursiv gesetzten Kriterien sind auch für die Messbarkeit der IT-Security relevant. Und im Hinblick auf diese Qualitätskriterien weisen die derzeit üblichen Ansätze etliche Defizite auf!

Die ISO 27001 stellt eine Empfehlung und ein Framework zur Erhöhung der Prozessreife in der IT-Sicherheit dar. Basierend auf der bereits angemerkten einfachen Messbarkeit der Prozessreife lag es nahe, dafür ein Zertifizierungssystem zu entwickeln. Die Qualitätsmessung der Sicherheit erfolgt jedoch binär: Man erhält ein Zertifikat oder eben nicht. Die im Automotive-Bereich üblich gewordene TISAX-Zertifizierung detailliert – aufsetzend auf der ISO 27001 – diese „Messung" in mehrere Stufen. Auch der „Quick Check" des versicherungsnahen VdS setzt an vielen Stellen auf die Ideen der ISO 27001 auf.

Alle diese Ansätze haben aber das Problem, dass sie die Prozessreife messen, nicht das Ergebnis – und damit am Problem vorbei messen (Stichwort: Relevanz). So listet etwa die Darknet-Präsenz der Conti-Nachfolgegruppe „Black Basta" aktuell einen anerkannten deutschen Cyber-Security-Dienstleister, der sogar selbst ISO-27001-Zertifikate ausstellt und Prüfungen vornimmt, als Opfer einer umfassenden Ransomwareattacke. Und auch sonst sind die Listen der „Hackergruppen" gemischt mit zertifizierten und nicht-zertifizierten Unternehmen befüllt. Das verdeutlicht, was aus der Qualitätsbetrachtung bereits klar wurde: Prozessreife allein schützt nicht vor Angriffen.

Um die grundlegenden Anforderungen an die Qualität einer Messbarkeit von Sicherheit zu erfüllen, ist die Messung der „realisierten Sicherheit" – also der Ergebnisqualität – das Maß der Dinge. Auch dazu gibt es bereits etliche Ansätze auf dem Markt: Die bekanntesten sind wohl Penetrationstests, Versicherungsfragebögen und Cyber-Ratingagenturen (Marktführer sind hier wohl die amerikanischen Unternehmen wie Bitsight und Security Scorecard, deutsche Unternehmen wären Cysmo und CyDIS). Dennoch gibt es auch hier Kritikpunkte:

Bei Penetrationstests kann es an Objektivität und Wiederholbarkeit mangeln: Beauftragt man einen zweiten Test (bzw. eine zweite Messung) bei einer unabhängigen Stelle, sollten eigentlich die gleichen Ergebnisse herauskommen. Penetrationstests und Red-Teaming-Aufträge sind aber sehr stark vom ausführenden IT-Sicherheitsexperten abhängig, sodass oft unterschiedliche Ergebnisse erzielt werden. Zudem zeigt ein Test per se nur die Anwesenheit von Fehlern, nicht aber deren Abwesenheit. Um die notwendige Abdeckung für eine aussagekräftige Messung zu erreichen, müssen umfangreiche Tests mit verschiedenen, klar definierten Zielen und Szenarien zum Einsatz kommen – das ist bei Penetrationstests personalintensiv und damit teuer.

Cyber-Ratingagenturen scheinen sich dieses Problems anzunehmen: Mit umfangreichen, hochautomatisierten Tests und Analysen wird versucht, ein Gesamtbild der IT-Sicherheit zu erstellen. Ziel ist dabei, teure Personalressourcen in die Gewinnung von gesamthaften Lagebildern zu stecken und dafür pro Test nur wenig oder gar keinen manuellen Aufwand zu erzeugen. Leider leidet bei den Ergebnissen oft die Nachvollziehbarkeit, das heißt die Messung und das Zustandekommen ihrer Ergebnisse sind oft nicht transparent. Hinzu kommt, dass die unvermeidlichen „False Positives" die Korrektheit der Messung negativ beeinflussen.

Bleiben noch die Versicherungsfragebögen, die angesichts der zunehmenden Angriffe im letzten Jahr deutlich weiterentwickelt worden sind. Hier fragt man zwar harte Fakten ab (z. B.. „Nutzen Sie MFA?") – „ja/nein"-Antworten sind jedoch oft zu oberflächlich, um ein ausreichend genaues Messergebnis zu produzieren (Stichwort: Validität).

Wie ginge es besser?

Um die Probleme der bisherigen Ansätze zu beheben, müssen Einschränkungen gemacht werden. Die wichtigste lautet, klar begrenzt ein bestimmtes Ziel der Verteidigung zu betrachten: Die Messung erfolgt dabei immer anhand einer in der Praxis vorkommenden Bedrohung. Dabei sind „Bedrohungen" nicht über den technischen Angriffsweg (Attack-Vector), sondern über die Täter (Threat-Actor) und ihre Motivation zu definieren.

Das Beispiel für die folgenden Ausführungen ist die – zugegebenermaßen einfachste – Kombination: organisierte Kriminalität mit der Motivation der Erpressung durch Denial-of-Service (Verschlüsselung von Daten) und drohender Kompromittierung (Exfiltration), sprich Ransomware. Für diese eingeschränkte Aufgabe lautet die Kernfrage jetzt: Wie baut man ein objektives, genaues und wiederholbares Messverfahren, das die Resilienz eines Unternehmens gegen heute gängige Ransomware-Attacken misst?

Analog zu anderen Messungen – beispielsweise der Trinkwasserqualität – benötigt man wohl etliche Messpunkte, um ein aussagekräftiges Bild zu erzeugen. Die Teilaufgaben für die Messbarkeit lauten daher:

- Definition einer Anzahl von *Messpunkten,* sodass eine umfassende Betrachtung aller zur Abwehr von Ransomware notwendigen Aspekte gewährleistet ist. Als Startpunkt dafür kann die Liste der 22 „unverhandelbaren Mindeststandards" dienen [2]. Jeder der Messpunkte muss sich an der realisierten Sicherheit orientieren, ein Ausweichen auf die Meta-Prozessebene ist nicht erlaubt! Die Messpunkte müssen alle relevant für die Bedrohung sein

und diese Relevanz wird auch verständlich und logisch argumentiert dargestellt.

- Definition eines *Messverfahrens* für jeden Messpunkt: Dieses Verfahren muss objektiv (idealerweise toolgestützt), überprüfbar (keine „Black Magic"), wiederholbar und genau sein. Die Messung muss von Dritten nachvollziehbar sein. Ein schönes Beispiel wäre die Messung der Active-Directory-Sicherheit mittels eines Pingcastle-Scans (www.pingcastle.com).

- Definition einer sinnvollen, verständlichen und nachvollziehbaren *Kombination* der Messpunkte zu einem Gesamtergebnis. Beispielsweise könnte man festlegen, dass wenn nur ein bestimmter Wert zu niedrig ist, andere aber sehr gut sind, das Ergebnis immer noch „ok" wäre.

Elementar wichtig ist bei all dem die nachweisbare Kausalität zwischen dem erreichten Schutz und dem gemessenen Ergebnis – diese Anforderung hat absolute Priorität 1!

Ein Nebenziel ist es, dass sich die Messungen (ggf. nach einer kleinen Schulung) von allen IT-affinen Personen mit dem gleichem Ergebnis durchführen lässt (Stichwort: Reliabilität) – und dafür eben kein ausgebildeter Cyber-Security-Experte notwendig ist. Denn die Messungen müssen sich in der Fläche und häufig durchführen lassen, ohne Behinderungen durch Personalengpässe.

Dabei ist klar: All das ist erstmal „nur" die Messung. Die gemessenen Daten können (und müssen) dann für die Projektierung geeigneter Verbesserungsmaßnahmen verwendet werden, die spezifisch an die entsprechende Organisation angepasst sind. Messergebnisse können aber auch als Basis für die Kalkulation eines möglichen Maximalschadens im Sinne einer Risikobewertung (z. B. durch Versicherer oder Auftraggeber) dienen. Für diese weiteren Schritte beöntigt man sicherlich einen erfahrenen Experten – Automatismen erscheinen hier nicht sinnvoll.

Woran hakts?

Die Erfüllung der genannten Qualitätskriterien in einem toolgestützen Messverfahren ist kein einfaches Unterfangen und wird sich in der Realität immer mit eingeschliffenen prozessorientierten Denkweisen in der IT-Sicherheit vergleichen lassen müssen. Daher ist es essenziell, die Messpunkte unumstritten aus der Bedrohung abzuleiten und bei den Messergebnissen möglichst wenig Spielraum für Interpretation zu lassen.

Ein analoges Beispiel wäre: Ein Auditor, der die Wasserqualität mit einem anerkannten chemischen Testverfahren analysiert und dann die Ergebnisse bereitstellt, ist keinerlei Diskussionen ausgesetzt. Es ist anschließend Aufgabe der Kommune, mit geeigneten Maßnahmen die gewünschte Wasserqualität herzustellen und einen erneuten Test zu beauftragen. Genau so muss das letztlich auch in der Cyber-Sicherheit funktionieren.

Vielleicht ist das nur ein unrealistischer Traum. Tatsache ist aber, dass uns die Bedrohungslage in der Cyber-Sicherheit zu neuen Ansätzen zwingt. Und hier gilt: Auf Veränderungen zu hoffen, ohne selbst etwas zu tun, ist wie am Bahnhof zu stehen und auf ein Schiff zu warten. Die Autoren haben sich daher für dieses Jahr zum Ziel gesetzt, für eine erste Bedrohung (Ransomware) ein solches Messverfahren zu definieren und zu veröffentlichen. Mitstreiter, die sich mit einbringen möchten, sind herzlich willkommen und werden gebeten sich per E-Mail an info@corporate-trust.de zu melden. Auch Hinweise (idealerweise mit einer kritischen Würdigung) auf weitere, bereits am Markt befindliche Messverfahren wären sehr wertvoll. ■

Dipl.-Inf. Florian Oelmaier ist Prokurist und Leiter IT-Sicherheit & Computerkriminalität, IT-Krisenmanagement, Falko Weiß ist Leiter Cloud-Security & Auditing, Arthur Naefe Leiter IT-Forensik & KI-Sicherheit bei der Corporate Trust Business Risk & Crisis Management GmbH.

Literatur

[1] Helmut Balzert, Marion Schröder, Christian Schäfer, Wissenschaftliches Arbeiten – Ethik, Inhalt & Form wissenschaftlicher Arbeiten, Handwerkszeug, Quellen, Projektmanagement, Präsentation, 3. Auflage, Prof. Balzert Stiftung, Juni 2022, E-Book als PDF verfügbar (CC BY-NC-ND) über z. B. https://dl.gi.de/handle/20.500.12116/38673

[2] Florian Oelmaier, Un-ver-zicht-bar! (Update), 22 technische Mindeststandards für 2022, <kes> 2022#1, S. 54