Threat-Driven Security (1)

Das Ende der Schutzbedarfsanalyse

Der Ausgangspunkt jeder Sicherheitsmethodik ist derzeit die Schutzbedarfsanalyse oder -feststellung. Dabei handelt es sich jedoch um eine Innenbetrachtung: Im Fokus stehen die eigenen „Kronjuwelen" (Asset-Driven Security). Eine solche Vorgehensweise ist heute jedoch nicht mehr zeitgemäß, warnt unser Autor und empfiehlt einen Wechsel in Richtung Bedrohungsanalyse.

Von Florian Oelmaier und Bernhard Mathar, München

Die Welt der IT-Sicherheit hat sich seit der Jahrtausendwende grundlegend verändert. Auf cve.mitre.org wurden im Jahr 2000 insgesamt etwa 1200 securityrelevante Bugs erfasst – 2017 waren es zehnmal so viele. Da der IT-Einsatz großflächiger, die Systeme komplexer und die Vernetzung intensiviert wurde, verwundert dieser Anstieg nicht. Betrachtet man die Situation qualitativ, zeigt sich ein anderes Bild: Ein Vergleich der Buglisten aus den Jahren 2000 und 2017 führt unweigerlich zu dem Schluss, dass die Lücken nicht schlimmer sind und die Software nicht unsicherer geworden ist – es gibt einfach nur mehr. Tatsache ist: Bereits 2000 lieferte die IT genug Möglichkeiten und Angriffsvektoren für die organisierte Kriminalität, für Industriespione und Regierungshacker. Dennoch hat die Bedrohungslage (unabhängig von den Fallzahlen) heute eine andere Qualität als vor 18 Jahren. Was aber macht diesen Unterschied aus?

Bedrohungen

Eine Bedrohung besteht immer aus drei Komponenten: Täter (bzw. Tätergruppe), Angriffsvektor/-methodik und Motivation. Erst wenn all diese Komponenten zusammenkommen, liegt eine echte Bedrohungssituation vor – fehlt eine der drei Komponenten, ist ein Angriff bestenfalls hypothetisch denkbar.

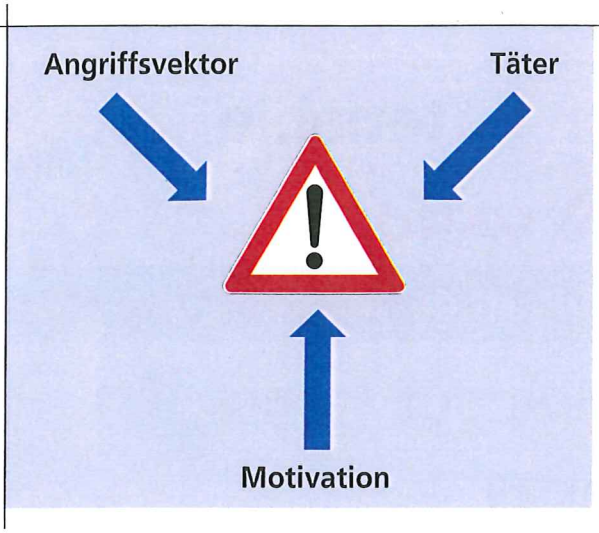

Abbildung 1: Eine Bedrohung besteht aus drei Komponenten.

Berücksichtigt man dieses Modell, wird der Unterschied in der Sicherheitslage zwischen 2000 und 2018 schnell deutlich: Waren es zu Beginn des Jahrtausends im Wesentlichen IT-Experten, Script-Kiddies und Technologiebegeisterte, die aus Spieltrieb, Geltungssucht und wegen der Herausforderung Attacken verübten, so stehen wir heute völlig neuen Tätergruppen mit ganz anderen Motiven gegenüber: Organisierte Kriminalität, Cybersöldner, Militäreinheiten und eventuell auch bald Terroristen sind unter den möglichen Tätern zu finden. Ihre Absichten sind vielfach ökonomischer Natur: Es geht um Geld und wirtschaftliche Vorteile – Erpressung, Betrug, Spionage und Sabotage. Auf der Metaebene sind dabei die Angriffsvektoren strukturell im Wesentlichen gleich geblieben.

Sicherheits-Bedarf

Gleichzeitig gilt eine alte Sicherheits-Weisheit noch immer: Wer alles schützt, schützt nichts. Schon vor Jahren hat sich die Überzeugung etabliert, dass es keinen idealen Einsatz der verfügbaren Ressourcen darstellt, alles in der IT gleichmäßig abzusichern. Stattdessen lautet das Motto, lieber einige Dinge weniger intensiv zu schützen, dafür andere umso mehr – eine abgestufte, bedarfsgerechte IT-Sicherheit ist das Ziel. Und seit jeher ist die Schutzbedarfsanalyse oder -feststellung das bewährte Werkzeug aller Sicherheitsexperten, wenn es um die Identifikation der wichtigsten Assets im Unternehmen geht – sie wurde auch bereits im letzten Jahrhundert im IT-Grundschutz des BSI verankert.

In einer Welt, in der Bedrohungen klar von „Technologen" ausgingen und die Motivation der Täter

(Spieltrieb, Geltungssucht) keinen Rückschluss auf ihre Angriffsziele zuließ, war dieses Werkzeug auch passend. Die Schutzbedarfsanalyse ist allerdings eine nach innen gerichtete Methode: Wir erfassen *unsere* Systeme und Daten, analysieren *unsere* Prozesse und erheben *unseren* potenziellen Schaden.

Trifft man damit immer die Motivation der möglichen Angreifer? Oder gibt es vielleicht doch Tätergruppen, die etwas anderes im Sinn haben und sich nicht an unserer Einschätzung orientieren? Spätestens im Rahmen von Internet-of-Things-(IoT)- oder Industrie-4.0-Projekten stößt die Schutzbedarfsanalyse an weitere Grenzen: Welchen Schutzbedarf müssen die von uns konstruierten Geräte beim Endkunden erfüllen? Meist zeigt die Analyse hier in allen Kategorien den höchsten Wert – damit ist eine Abstufung der Absicherung nicht mehr möglich.

Blick nach außen

In dieser neuen und komplexen Welt müssen die Sicherheitsverantwortlichen ihren Blick nach außen richten: Welche Tätergruppen gibt es? Welche davon haben ein Motiv, unser Unternehmen anzugreifen? Was genau motiviert sie? Wie könnten sie vorgehen?

Basierend auf diesen Informationen kann man dann eine zielgenaue Verteidigungsstrategie entwerfen. Kernpunkt bleibt dabei weiterhin die Reduktion der Angriffsmöglichkeiten durch technische, organisatorische oder personelle Gegenmaßnahmen. Dennoch darf sich ein Verteidigungskonzept heute nicht mehr ausschließlich nach innen richten, sondern muss auch an Täter und Motivation denken.

Mögliche Elemente einer Verteidigungsstrategie sind:

- Reduktion der Täterkreise durch Verfolgungsdruck und Abschreckung (z. B. durch Zusammen-

Täter bzw. Tätergruppe	Motivation	Angriffsvektor (Beispiele)
organisierte Kriminalität	direkt Geld abgreifen	• Fake-President o. Ä. • Social-Engineering auf Firmenebene
Mitarbeiter	Geld	• Geldüberweisungen tätigen bzw. umschreiben • Kredit ohne Vorprüfung anlegen und Überweisung tätigen
Insider	finanzieller Vorteil	• Weitergabe vertraulicher Informationen an Behörden
Insider	Vergeltung/Rache finanzieller Vorteil	• legitime Zugriffsmöglichkeit auf Systeme oder Daten
organisierte Kriminalität	direkt Geld abgreifen	• APT-Angriff im Stil von Carbanak • manuelle Prozessanpassung der Dauerüberweisungen (Login bekannt, erbeutet), um kleine Beträge abzuzweigen • SWIFT-Nachrichten (meist Text- bzw. XML-Dateien) anpassen (Geldtransfersysteme, Übertragungsweg) • Kredit ohne Vorprüfung anlegen und Überweisung tätigen
Mitarbeiter Dienstleister	unabsichtlich Fahrlässigkeit	• Fehlbedienung von Systemen/Applikationen
Mitarbeiter ehemaliger Mitarbeiter organisierte Kriminalität Terroristen	Erpressung Rufschädigung finanzieller Vorteil	• Ausspähen von Zugangsdaten • Manipulationen im Zahlungsverkehr
Whistleblower	ethisch-moralische Beweggründe	• Weitergabe vertraulicher Informationen an Behörden oder Journalisten
Ermittlungsbehörden (Staatsanwaltschaft, Polizei, Steuerfahndung, ...)	Auftrag	• Observation • verdeckte Ermittlungen (Social-Engineering) • Telefonüberwachung, Wanzen, Lauschangriff
organisierte Kriminalität	Geld erpressen	• Androhung/Durchführung eines Denial-of-Service-Angriffs (DoS)
Medien und investigative Journalisten	Schlagzeilen	• Social-Engineering
ehemaliger Insider	Vergeltung/Rache	• von außen nutzbare Zugänge und Schwachpunkte in Geschäftsprozessen
Mitarbeiter ehemaliger Mitarbeiter	Karrierevorteil finanzieller Vorteil	• Missbrauch externer Dienste
unzufriedener Mitarbeiter ehemaliger Mitarbeiter	Rufschädigung	• Datenschutzverletzungen öffentlich machen
Mitbewerber	Wettbewerbsvorteil	• Abwerben von Schlüsselmitarbeitern
Hacker	Spielen mit Systemen Aufdecken von Schwachstellen	• extern erreichbare Dienste/Systeme
organisierte Kriminalität	Geld erpressen	• Ausspähen von vertraulichen Informationen

Tabelle 1: Beispiel für die Bedrohungsanalyse für eine Bank

arbeit mit Behörden oder Erhöhung der Entdeckungsmöglichkeiten)

_____ Reduktion der Motivation durch Einbindung (z. B. durch Bug-Bounty-Programme)

_____ Voraufklärung von Täterkreisen (z. B. durch Überwachung einschlägiger Foren)

Um diesen Blick über den Tellerrand zu schärfen, darf der Startpunkt der Sicherheit nicht mehr alleine eine nach innen gewandte, von den eigenen Werten getriebene Schutzbedarfsanalyse sein. Am Anfang aller Sicherheitsanstrengungen muss vielmehr eine systematische Analyse der Bedrohungslage stehen. Das Credo lautet also: Weg von der Asset-Driven Security und hin zur Threat-Driven Security.

Bedrohungs-Analyse

Eine Bedrohungsanalyse trägt die möglichen Kombinationen aus Täter, Motivation und Angriffsvektor(en) konkret zusammen. Danach erfolgt ein Rating der Bedrohungen, in dem man die einzelnen Bedrohungsszenarien gemäß ihrer Priorität ordnet. Eine beispielhafte Bedrohungsanalyse für eine Bank zeigt Tabelle 1.

Typischerweise werden in einem ersten Schritt Listen relevanter Täter beziehungsweise Tätergruppen erstellt – oft hilft es, den einzelnen Tätergruppen bereits konkrete Motivationen zuzuordnen. Danach ordnet man jeder möglichen Tätergruppe systematisch alle infrage kommenden Motivationen zu. So entsteht eine sortierte Liste aus Tätern und Motivationen (n-zu-m-verknüpft). Anschließend wird jedem solchen Tupel ein typischer Angriffsvektor beziehungsweise eine typische Angriffsart zugeordnet.

Diese letzte Zuordnung kann dabei nie vollständig sein: Denn ein Täter mit einer bestimmten Motivation wird immer wieder neue Angriffsvektoren versuchen, um an sein Ziel zu gelangen. Dennoch wird die Bedrohungsanalyse bereits durch die Zuordnung bespielhafter Angriffsvektoren greifbarer.

Im nächsten Schritt werden die Bedrohungen priorisiert: Der Vorteil dabei ist, dass sie auch von Mitarbeitern verstanden werden, die sich bislang nicht mit Cybersicherheit beschäftigt haben. Dementsprechend kann die Priorisierung leicht auf eine breite Basis gestellt werden. Das geschieht entweder im Umlaufverfahren („bitte in eine Reihenfolge der Gefährlichkeit bringen") oder im Team (z. B. mittels Planning-Poker-Karten).

Abschließend teilt man die Szenarien anhand der vorherigen Einschätzungen drei Kategorien zu:

_____ *akut:* Szenarien, bei denen es wahrscheinlich ist, dass sie aktuell passieren können

_____ *aufstrebend:* Szenarien, die im Feld beobachtet werden, aber aufgrund der Situation derzeit eher unwahrscheinlich sind

_____ *Außenseiter:* Szenarien, die in der Praxis noch nicht vorkommen oder relevant sind, es aber zukünftig werden können

Fazit

Der Anfangspunkt jeder Sicherheitsmethodik ist derzeit fast immer eine Schutzbedarfsanalyse. Dabei handelt es sich jedoch um eine Innenbetrachtung: Im Fokus stehen die eigenen „Kronjuwelen" (Asset-Driven Security). Spätestens im Bereich von Internet of Things und Industrie 4.0 greift diese Betrachtung zu kurz. Eine Schutzbedarfsanalyse liefert hier ständig höchste Werte für alle Grundwerte der IT-Sicherheit – eine bedarfsgerechte Sicherheit lässt sich auf dieser Basis nicht entwerfen.

Um wieder zu einer abgestuften Sicherheitsbetrachtung zu kommen, muss sich die Basis unserer Betrachtung ändern: Statt die eigenen Assets in den Kategorien Vertraulichkeit, Integrität und Verfügbarkeit in Risikoklassen einzustufen, sollte man eine Liste von Bedrohungen für das zu bewertende IT-System erstellen (Threat-Driven Security).

Eine Bedrohung besteht dabei immer aus drei Komponenten: Angriffsvektor, Täter und Motivation. Anschließend erfolgt eine Einordnung der jeweiligen Bedrohung in Wahrscheinlichkeitsklassen. Auf dieser Grundlage lassen sich sowohl eine angemessene Sicherheitsstrategie entwickeln als auch die Angemessenheit der Sicherheit beurteilen. ■

Dipl.-Inf. Florian Oelmaier ist Leiter, Bernhard Mathar stellvertretender Leiter IT-Sicherheit und Computerkriminalität bei der Corporate Trust – Business Risk & Crisis Management GmbH.

Im zweiten Teil dieses Beitrags beschreiben die Autoren, was Threat-Driven Security für ein modernes Sicherheitsteam bedeutet, und zeigen neue Ansätze für die Organisation einer Sicherheitsabteilung auf.