IKT-Risikoanalyse am Beispiel APT

Stefan Schiebeck[1] · Martin Latzenhofer[1] · Brigitte Palensky[1]
Stefan Schauer[1] · Gerald Quirchmayr[2] · Thomas Benesch[3]
Johannes Göllner[4] · Christian Meurers[4] · Andreas Peer[4]

[1]Austrian Institute of Technology – Digital Safety & Security Department
{stefan.schiebeck.fl | martin.latzenhofer
brigitte.palensky | stefan.schauer}@ait.ac.at

[2] Universität Wien – Fakultät für Informatik
gerald.quirchmayr@univie.ac.at

[3]s-benesch – Research & Development
thom@s-benesch.com

[4] Bundesministerium für Landesverteidigung und Sport
{johannes.goellner | christian.meurers | andreas.peer}@bmlvs.gv.at

Zusammenfassung

Die Bedrohung durch Advanced Persistent Threats (APT) hat im vergangenen Jahrzehnt vermehrt zugenommen und APTs sind seitdem Auslöser für eine markante Zahl an kritischen Sicherheitsvorfällen weltweit. Ein Hauptgrund dafür ist die Tatsache, dass bei APTs nicht nur eine Sicherheitslücke in einem System ausgenutzt wird, sondern dass durch eine verkettete Reihe von Lücken in unterschiedlichen Bereichen des Systems ein entsprechend großer Schaden angerichtet werden kann. Im Rahmen des KIRAS-Projekts „MetaRisk – Meta-Risiko-Modell für kritische Infrastrukturen“ wurde ein ganzheitliches Modell für die Risikoanalyse von Organisationen definiert. Über dieses Modell ist es möglich, nicht nur die angesprochenen Sicherheitslücken über die einzelnen Bereiche einer Organisation hinweg zu identifizieren, sondern Zwischenfälle auch entsprechend zu modellieren und zu bewerten. Der vorliegende Beitrag beschreibt die Anwendung des MetaRisk-Modells auf einen fiktiven APT-Angriff auf einer globalen Ebene und diskutiert mögliche Gegenmaßnahmen.

1 Einleitung

Obwohl im Bereich der Informationssicherheit interne Angreifer mittlerweile als die größere Bedrohung angesehen werden [Cole00], wird in der Praxis weiterhin hauptsächlich auf Perimeter Control gesetzt. In den inneren Bereichen, etwa der Demilitarized Zone (DMZ) oder dem Intranet, werden zwar, gemäß technischer Empfehlungen [Sans00], ebenso logische Unterteilungen der Netzwerke mit unterschiedlichen Sicherheitsanforderungen implementiert, allerdings nimmt die Intensität der Überwachung merklich ab. Intrusion-Detection- sowie Intrusion-Prevention-Systeme erfordern ein hohes Maß an Beschäftigung, Pflege und Administration und binden Ressourcen. Genau diesen Wechsel der Bedrohungslage von außen nach innen machen

P. Schartner · K. Lemke-Rust · M. Ullmann (Hrsg.) · D•A•CH Security 2015 · syssec (2015) 145-158.

sich neuartige Angriffe, insbesondere sogenannte Advanced Persistent Threats (APTs), zunutze.

Die Bezeichnung APT steht für einen hochentwickelten („advanced“), auf eine lange Zeitspanne angelegten („persistent“) Angriff auf ein Computer-Netzwerk. Die Angreifer verfügen über große Ressourcen und setzen das volle Spektrum an digitalen, physischen und sozialen Angriffsvektoren ein. Der Angriff wird individuell auf eine spezifisch ausgewählte Opfer-Organisation zugeschnitten, wodurch konventionelle IT-Sicherheitsmaßnahmen erfolgreich unterlaufen werden und die Angreifer lange Zeit unentdeckt bleiben. Zudem kommt bei APTs zumeist Social Engineering zu Einsatz, um die menschlichen Schwachstellen in einem System auszunutzen. Mögliche Gegenmaßnahmen, wie etwa eine Verbesserung der „Awareness“ bezüglich der vorhandenen Gefahren von IKT-Systemen, werden aber kaum durchgeführt. So bieten laut einer Studie [Pone14] rund 52 % der Unternehmen keine entsprechenden Schulungen für ihre Mitarbeiter an.

Neben dem bekanntesten Beispiel einer APT-Attacke, dem Einsatz der Schadsoftware Stuxnet zur Sabotage der iranischen Nuklearanlagen, sind mittlerweile eine Reihe von weiteren APT-Attacken bekannt geworden, z.B. Operation Aurora, Shady Rat, Red October oder MiniDuke [MILP14][Tank11][FSSF15]. Wie der Mandiant-Report exemplarisch zeigt [Mand13], werden APTs bereits auf globaler Ebene eingesetzt und einzelne Angreifer stehen dabei in enger Verbindung zu staatlichen Organisationen. Der frühere Direktor des US Cyber Commands, General Keith Alexander, hat die chinesische Wirtschaftsspionage und den seit 2006 rasant zunehmenden elektronischen Diebstahl geistigen Eigentums der USA sogar als “den größten Wohlstandstransfer der Geschichte“ bezeichnet [Comm13]. Aus europäischer Sicht haben vor allem die Enthüllungen von Edward Snowden [Gree14] großes Aufsehen erregt. Geht man von den aktuellen Zahlen aus dem Bereich der Computerkriminalität aus [Bmi13][Inte13], ist es erschütternd, wie wenig entwickelt offenbar heutige Gegenmaßnahmen sind trotz der immer größer werden Anzahl von Attacken und des Schadens, den sie anrichten.

In diesem Paper werden die Rahmenbedingungen und Ergebnisse einer APT-Case Study beschrieben und die Bedrohungen von IT-Infrastrukturen in einen Gesamtzusammenhang gesetzt. In diesem Kontext wird ein organisationsweites Risikomodell präsentiert, welches im Rahmen des KIRAS-Projekts MetaRisk entwickelt wurde und das eine Methode zur Früherkennung von APTs durch eine strukturelle Bewertung der durch Kaskadeneffekte entstehenden Risiken ermöglicht. Hierfür wird im Abschnitt 2 auf die Rahmenbedingungen der Case Study eingegangen und der Lebenszyklus eines APTs anhand des Mandiant-Reports [Mand13] exemplarisch dargestellt. Abschnitt 3 beschreibt das entwickelte Modell zur unternehmensweiten Betrachtung und Bewertung des Risikos. In Abschnitt 4 wird die Anwendung des Modells auf die Case Study dargestellt. Im Abschnitt 5 werden die Vorteile und Grenzen des gewählten Ansatzes diskutiert und abschließend die Ergebnisse zusammenfasst.

2 Case Study Mandiant-Report

Der Mandiant-Report [Mand13] wurde im Rahmen des Projekts „MetaRisk – Meta-Risiko-Modell für kritische Infrastrukturen“ als Use-Case zur Veranschaulichung des entwickelten Modells herangezogen. Das Hauptziel des Projekts ist die Konzeption eines sensor-unterstützten Risikoanalyse- und Risikomanagementsystems, das auf einem generischen Modell einer Organisation aufbaut. Hierbei liegt der Fokus nicht nur auf dem Kontext der IKT-Strukturen,

sondern auf einer ganzheitlichen Beschreibung des Systems. Dadurch werden neben den technischen Bedrohungen auch weitere Risikopotentiale (wie etwa der oben genannte Faktor Mensch) identifiziert und in der Risikoanalyse bewertet. Das Projekt MetaRisk wird durch das KIRAS-Programm der österreichischen Forschungsförderungsgesellschaft (FFG) gefördert (Projekt-Nr. 840905). Beteiligt sind das Austrian Institute of Technology (als Projekt-Koordinator), die Universität Wien (Forschungsgruppe Multimedia Information Systems), das Bechtle IT-Systemhaus Österreich, das Institut für empirische Sozialforschung (IFES) sowie die IFES Feld. Als Bedarfsträger sind das Bundesministerium für Inneres (BM.I) und das Bundesministerium für Landesverteidigung und Sport (BMLVS, Abteilung für Zentraldokumentation und Information, Referat Wissensmanagement in der Landesverteidigungsakademie Wien) involviert.

2.1 Rahmenbedingungen

Im Februar 2013 erfolgte die Veröffentlichung eines Berichts des US-amerikanischen IT-Sicherheitsunternehmens Mandiant, das seit 2004 APT-Vorfälle auf der ganzen Welt beobachtet [Mand13]. In dem umfassenden Bericht beschreibt Mandiant seine Untersuchungsergebnisse bezüglich einer chinesischen Cyber-Spionage-Gruppe, von Mandiant „APT1“ genannt. Der Bericht belegt, dass diese Gruppe in Shanghai in einem Gebäude der chinesischen Volksbefreiungsarmee residiert, und Mandiant beschuldigt die chinesische Regierung explizit, direkt hinter dieser Gruppe zu stehen und gezielt Informationen von US- und anderen englisch-sprachigen Unternehmen zu erbeuten. Der Bericht liefert darüber hinaus eine Reihe von konkreten Daten bezüglich der Dimensionen des Schadens, den APT-Attacken anrichten können. Laut dem Bericht ist die Gruppe seit dem Jahr 2006 in mindestens 141 Organisationen eingedrungen und hat dort Terabytes an Daten gestohlen (siehe [Mand13], Seite 20-24).

2.2 Lebenszyklus einer APT-Attacke

Der Mandiant-Report beschreibt die Vorgehensweise der Angreifer in den prototypischen Phasen einer APT-Attacke, wodurch sich Möglichkeiten zur Abwehr ergeben (siehe Abbildung 1).

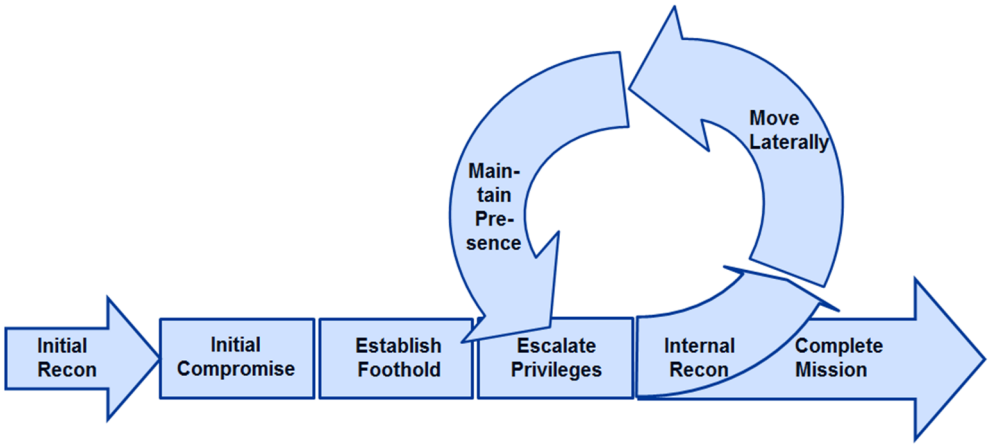

Abb. 1: Der Lebenszyklus eines APT-Angriffs. Quelle: [Mand13] S. 27.

1. **Initial Recon**: Im ersten Schritt des Lebenszyklus einer APT-Attacke erfolgt eine Auskundschaftung des anvisierten Systems, wobei gezielt nach Schwachstellen technischer oder menschlicher Natur (Social Engineering) gesucht wird. Zumeist sind es einzelne Mitarbeiter, die als vielversprechendste Eintrittspunkte ins Netzwerk identifiziert werden.

2. **Initial Compromise**: In der Phase der initialen Kompromittierung ist Spear-Phishing eine gängige Methode. Bei dieser Art der Social-Engineering-Attacke werden individuell kreierte, äußerst glaubhafte E-Mails versendet, die den Empfänger verleiten, auf einen bösartigen Anhang, einen Link zu einer Datei oder einer Webseite mit Malware zu klicken.
3. **Establish Foothold**: Sobald der Angreifer einen ersten Zugriff erreicht hat, versucht er diesen aufrechtzuerhalten und auszubauen. Gewöhnlich wird ein Remote-Access-Trojaner auf einem Host des Systems installiert, wobei versucht wird die Spuren zu verwischen oder zu überdecken. Auf diese oder eine ähnliche Weise wird ein Backdoor erstellt.

Die folgenden vier Schritte werden in der Regel mehr als einmal durchlaufen, solange bis sich der Angreifer zurückzieht, da er sein Ziel erreicht hat, oder bis er entdeckt wird.

4. **Escalate Privileges – Internal Recon – Move Laterally – Maintain Presence**: Als nächstes versucht der Angreifer durch Auskundschaften des Netzwerks gültige Benutzerrechte zu erlangen und seine Privilegien bis hin zu Administrationsrechten auszudehnen. Danach bewegt sich der Eindringling praktisch frei durch das gesamte Netzwerk. Er sucht und sammelt Informationen, etabliert weitere Backdoors und installiert betrügerische Utilities, um seine Aktivitäten nachhaltig weiter auszuführen und gleichzeitig zu verbergen.
5. **Complete Mission**: In der letzten Phase hat der Angreifer das eigentliche Ziel seiner Attacke erreicht. Zumeist ist das der Diebstahl von Daten in Form von geistigem Eigentum, Geschäftsverträgen, strategischen und politischen Dokumenten, etc. Die Daten werden auf einem Host gesammelt, komprimiert, verschlüsselt und dann möglichst unauffällig auf digitalem oder physischem Wege abtransportiert.

2.3 Schaden und Abwehr von APTs

Der Schaden, den die Cyber-Kriminalität weltweit anrichtet, ist enorm, und die Situation verschlimmert sich mit der zunehmenden Vernetzung aller Bereiche [Brew14]. APTs sind die momentan komplexeste Form solcher Angriffe. Bei den bekannt gewordenen APT-Attacken hat es Monate bis Jahre gedauert, bis die Opfer bemerkt haben, dass sie kompromittiert wurden [Brew14][Mand13]. Die betroffenen Organisationen stammen aus unterschiedlichen Bereichen, wie etwa dem Energiesektor, IT und Kommunikation, klassische Industrien, Rüstung, Transport, Gesundheitswesen oder dem öffentlichen Sektor [Brew14] [Mand13] [Tank11] [MILP14]. Auf der Liste der Opfer finden sich Organisationen wie Sony, Google, RSA Security, Morgan Stanley und der Internationale Währungsfonds [Tank11].

Angesichts der praktischen Unmöglichkeit, ein erfolgreiches Eindringen bei gezielten Attacken zu verhindern, stellt die Detektion von Angriffen eine erfolgversprechende Alternative dar. Auch wenn APT-Angriffe schwierig zu identifizieren sind und die Angreifer das Verhalten der normalen User ausspionieren und kopieren, so hinterlassen sie doch immer Spuren [Tank11][Brew14]. Essentiell für das Finden dieser Spuren ist das Wissen über die „normalen“ Aktivitätsmuster in einem Netzwerk und das Verständnis, wie einzelne Ereignisse im Zusammenhang zueinander stehen. Hierfür können z.B. Anomaly Detection Systeme [FSSF15] eingesetzt werden, die Daten aus Supportsystemen wie etwa Network-Intrusion-Detection, Antivirus-Installationen oder Firewall Logs extrahieren und aufgrund von vordefiniertem oder selbständig gelerntem Wissen Korrelationen zwischen einzelnen Ereignissen herstellen. Angesichts der Kombination aller möglichen Angriffsvektoren erfordert die Detektion von APTs darüber hinaus aber eine Abbildung der gesamten Organisation und die Installation von Kontrollprozessen für alle relevanten Bereiche. Diese müssen effektive und zeitnahe Berichtsmechanismen

besitzen. Die kontinuierliche Überwachung aller Kontrollprozesse und die Analyse der erstellten Berichte helfen nicht nur, Anomalien zu entdecken und rasch Alarme auszulösen, sondern tragen auch zur Identifikation von noch vorhandenen Sicherheitslücken bei.

3 Modellbeschreibung

In [Schi14] wurde die ISO/IEC 27001, der internationale Standard für Informationssicherheit sowie die entsprechende Risikomanagement-Erweiterung ISO/IEC 27005 [Isoi11] um die iterative Integration von Kennzahlen, Indikatoren und Expertenwissen sowie der Möglichkeit der Automatisierung durch Sensoren erweitert (siehe Abbildung 2) und in Form eines Prototypen evaluiert. Diese Arbeit wurde im Zuge des KIRAS-Projekts MetaRisk um Modelle zur Organisationssteuerung und -planung, sowie um einen graphenbasierten Ansatz zur Darstellung von komplexen Zusammenhängen in schemafreier Form erweitert (s. Abschnitt 3.2).

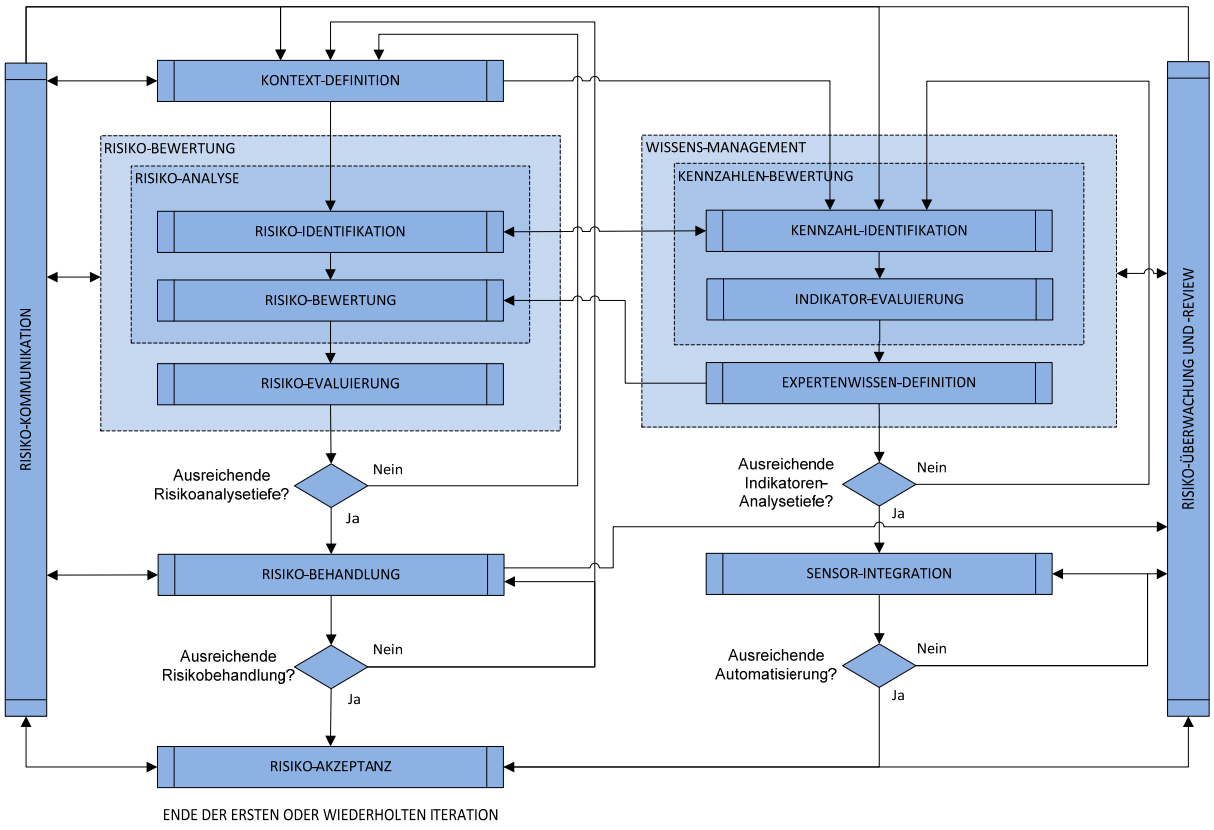

Abb. 2: Erweiterter ISO/IEC 27005 Risikomanagement-Prozess [Schi14]

Im Zuge des in Abbildung 2 angeführten Risikomanagementprozesses werden zur Risikoidentifikation und Risikobewertung die nachstehend beschriebenen Analyseschritte (s. Abschnitt 3.1) iterativ durchlaufen. Sämtliche im Unternehmen verfügbaren risikorelevanten Kennzahlen und Events können ebenfalls wiederholend in die kontinuierliche Risikobewertung integriert werden, indem diese als Kennzahlen identifiziert und mit Hilfe von Indikatoren evaluiert werden. Formal definiertes Expertenwissen stellt die kontinuierliche Anpassung der mit den Indikatoren korrespondierenden Risikofaktoren sicher, wobei die Entwicklung und der Einsatz von Sensoren zur Sammlung der Kennzahlen eine vollständige Automatisierung ermöglicht.

3.1 Analysemodell

Der hier vorgestellte Ansatz baut auf den BSI IT-Grundschutz-Standards, -Katalogen und -Kreuzreferenzen [Bsi00a][Bsi00b] auf und erweitert diese u.a. um die Sicht auf Schutzbedürfnisse (z.B. Risikodimensionen wie Vertraulichkeit, Integrität) und Risikomanagementaspekte. Abbildung 3 stellt die verschiedenen Analyseebenen des Modells graphisch dar.

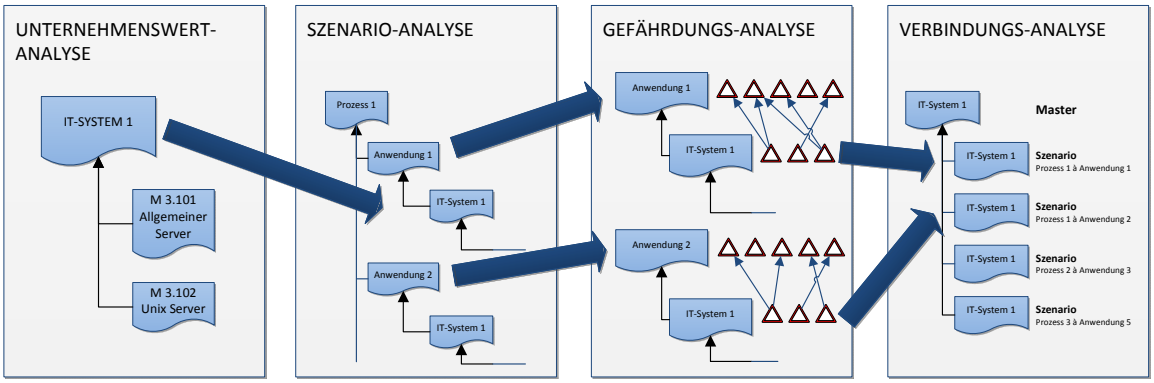

Abb. 3: Analyseebenen des Modells

- **Unternehmenswertanalyse:** Hier werden Unternehmenswerte basierend auf der Struktur von IT-Grundschutz erhoben und durch die Zuordnung eines oder mehrerer IT-Grundschutz-Module beschrieben. Es können aber auch rechtliche Entitäten, Prozesse, Organisationseinheiten etc. in gleicher Weise dargestellt werden. Die in den BSI Kreuzreferenzen enthaltenen Informationen (Verknüpfung von Gefährdungen mit Schutzmaßnahmen) dienen in Verbindung mit organisationsspezifischen Anpassungen dazu, Exponierungen (Maß für die Angriffsfläche) für die Unternehmenswerte und deren Schutzbedürfnisse zu berechnen.
- **Szenarioanalyse:** Im Zuge der Szenarioanalyse können die Abhängigkeiten und die damit verbundene Risikovererbung von Unternehmenswerten ermittelt werden. Daraus kann eine Business Impact Analyse (BIA) abgeleitet werden, um die Schutzbedürfnisse der Unternehmenswerte in den unterschiedlichen Szenarien zu identifizieren.
- **Gefährdungsanalyse:** Diese Abhängigkeiten, welche eine High-Level-Risikovererbung zwischen den Komponenten auf Schutzbedarfsebene ermöglichen, stellen den Ausgangspunkt für eine optionale Low-Level-Darstellung der aufeinander wirkenden Gefährdungen (Gefährdungsanalyse) zwischen bereits strukturierten Komponenten dar.
- **Verbindungsanalyse:** Am Ende jeder Berechnungsrunde erfolgt die Aggregation sämtlicher Szenarios pro Unternehmenswert, um generalisierte Risiken sowie maximale Schutzbedürfnisse für jeden Unternehmenswert darstellen zu können.

3.2 Graphenmodell

Das im Zuge des Projekts MetaRisk entwickelte Modell zur Modellierung und Berechnung der Risikoobjekte ist in Abbildung 4 als graphenbasiertes Meta-Modell dargestellt. Graphendatenbanken sind besonders bei Traversierung von Graphen (erfolgt oft in Echtzeit), dem Finden von Nachbarn und bei Topologieanalysen effizienter als relationale Modelle. Des weiteren sind Graphendatenbanken flexibler bei Veränderungen von Strukturen [UrMy15].

Vorhandene Risikoinformationen werden einem Risikomodell (*Risk Model*) zugeordnet, welches die Ziele, Grenzen und Anforderungen narrativ beschreibt. Dem Risikomodell sind auch Benutzer zugeordnet (*Risk Model requires User*) entsprechend ihrer rollenspezifischen Verantwortlichkeiten (*User described_by Role*) für die Planung oder Implementierung der benötigten Sicherheitsmaßnahmen (*Role responsible_for Safeguard*).

Ein wichtiger Schritt ist die Zuordnung von Zielen (*Risk Model defines Goals*) zum Risikomodell. Als sinnvolle Taxonomie zur Zieldefinition eignet sich insbesondere die Typisierung von IT-Grundschutz mit einer Unterscheidung in Modul-Typen (Anwendungen, IT-Systeme, Netze, Infrastruktur, Übergeordnete Aspekte), Gefährdungs-Typen (Elementare Gefährdungen, Höhere Gewalt, Organisatorische Mängel, Menschliche Fehlhandlungen, Technisches Versagen, Vorsätzliche Handlungen) und Maßnahmen-Typen (Infrastruktur, Organisation, Personal, Hardware und Software, Kommunikation, Notfallvorsorge). COBIT-spezifische Ziele und Anforderungen (Stakeholder Needs, Enterprise Goals, IT-related Goals, etc.) können durch Kreuzreferenzen von COBIT 5 mit IT-Grundschutz ebenfalls herangezogen werden. Die definierten Ziele korrelieren mit den jeweiligen Exponierungen der Komponenten im Risikomodell und wirken auf Risikodimensionen (z.B. Vertraulichkeit) und deren spezifische Schutzbedürfnisse (*translate_to Protection Criteria*), welche separat auswählbar sind (*Risk Model analyses Protection Criteria*).

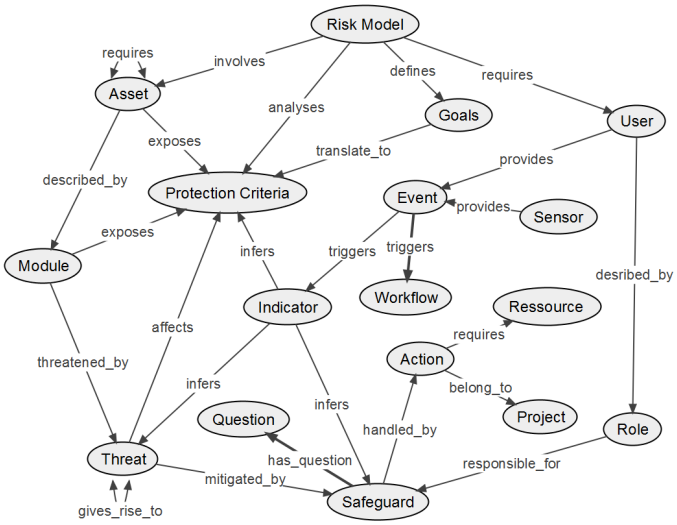

Abb. 4: Graphenbasiertes Meta-Modell

Essentiell für das Risikomodell ist die Zuordnung von Unternehmenswerten (*Risk Model involves Asset*). Diese werden durch IT-Grundschutz-Module (*Modules*), Gefährdungen (*Threats*), Sicherheitsmaßnahmen (*Safeguards*) und Rollen (*Roles*) dargestellt. Exponierungen werden für Unternehmenswerte, Module und Gefährdungen getrennt modelliert (*Asset/Module/Threat exposes Protection Criteria*) und gespeichert. Unternehmenswerte können im Zuge der Szenarioanalyse miteinander verknüpft werden (*Asset requires Asset*), um ihre Abhängigkeiten darzustellen. Ein weiterer möglicher Schritt ist die Durchführung einer Gefährdungsanalyse. Dabei werden Gefährdungskaskaden (*Threat gives_rise_to Threat*) zwischen den Gefährdungen der vorstrukturierten Unternehmenswerte modelliert.

Sowohl die Benutzer (*User*) als auch die automatisierbaren Sensoren (*Sensor*) können Events und Kennzahlen an das Framework liefern (*provide Event*), welche in Form von Indikatoren

und mit Hilfe von Expertenwissen (*triggers Indicator*) auf ihre korrespondierenden Risikofaktoren zurückgeführt werden. Dabei kann es sich um Schutzbedürfnisse (*infers Protection Criteria*), also Indikatoren mit Bezug auf den geschätzten Schaden, Gefährdungen (*infers Threat*), also Indikatoren mit Bezug auf Eintrittswahrscheinlichkeiten oder Sicherheitsmaßnahmen (*infers Safeguard*), also Indikatoren mit Bezug auf die Ausnutzbarkeit von Schwachstellen handeln.

Events können Workflows auslösen (*Event triggers Workflow*), z.B. um die im Rahmen von Schwachstellen-Scans neu identifizierten IT-Systeme in das Risikomodell zu integrieren. Zur Modellierung von Risikomanagement-Tätigkeiten werden ebenfalls Aktivitäten (*Safeguard handeled_by Action*) eingeführt, welche mit Ressourcen (z.B. Personal, Finanzen) und Projekten verknüpft werden können. Die Hinterlegung von Prioritäten, Kosten und Verfügbarkeiten ermöglicht die Nutzung von Funktionalitäten von Return-On-Security-Investment-Modellen.

Eine Erweiterung des generischen Meta-Modells ist aufgrund der schemafreien Definition im Kontext einer Graphendatenbank problemlos möglich. Die üblicherweise in Standard-Software benötigte Anpassung des Business-Codes zur Erweiterung der Analysefunktionalität wird größtenteils durch die Funktionalität der Graphen-Abfragesprache CYPHER [Neoj00] kompensiert, so können Analysemodelle mit erweiterten Anforderungen effizient implementiert werden.

3.3 Integration in ein Meta-Risiko-Gesamtmodell

Die IKT-spezifische Risikobetrachtung kann anschließend in ein unternehmensweites Meta-Risiko-Gesamtmodell integriert werden. Damit steht diese Information auch als Input für strategische Entscheidungen zur Verfügung, die durch ein Vorgehensmodell aufbereitet werden können. Im Projekt MetaRisk kam dabei das Z-Vorgehensmodell von [GöKM15] zur Anwendung (siehe Abbildung 5).

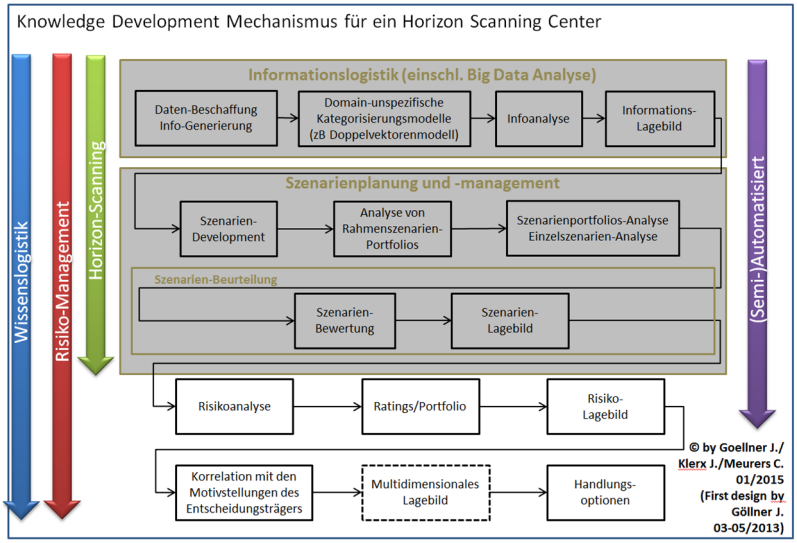

Abb. 5: Z-Vorgehensmodell [GöKM15]

Dieses liefert wichtige Bestandteile in der Informationslogistik, welche dann in die Szenarienplanung und das Szenarienmanagement einfließen. Eine Risikoanalyse, die auf den Ergebnissen des zuvor durchgeführten Horizon Scans basiert, bildet die Grundlage für Entscheidungsfindung von Handlungsoptionen auf strategischer, operativer und taktischer Ebene. Eine detaillierte Beschreibung der Komponenten des Z-Vorgehensmodells findet sich in [GöKM15]. Ein

Einbau in eine Kennzahlenlogik wäre z.B. anhand eines Knowledge Performance Monitoring Systems, wie in [WoMG10][GöKW10] gezeigt, möglich.

4 Anwendung auf das Szenario

Um das im Mandiant-APT1-Report vorgestellte Szenario zu simulieren, wird im Folgenden eine fiktive Organisation mit ihren Systemkomponenten dargestellt und potentielle darauf ablaufende Kaskadeneffekte analysiert. Dazu werden die Unternehmenswerte aus Abbildung 6 mit Hilfe von IT-Grundschutzmodulen dargestellt (Unternehmenswertanalyse) und die Abhängigkeiten zwischen den Unternehmenswerten mit Hilfe der Szenarioanalyse bestimmt. Die fiktive Organisation *Biomedical Research* betreibt vier Forschungslaboratorien mit steigenden Sicherheitsanforderungen (Biosafety Level 1-4) in physisch getrennten Räumlichkeiten, wobei diese ein im lokalen Gebäude zentrales Rechenzentrum sowie als gespiegeltes Backup ein im entfernten Verwaltungsgebäude gelegenes weiteres Rechenzentrum besitzen.

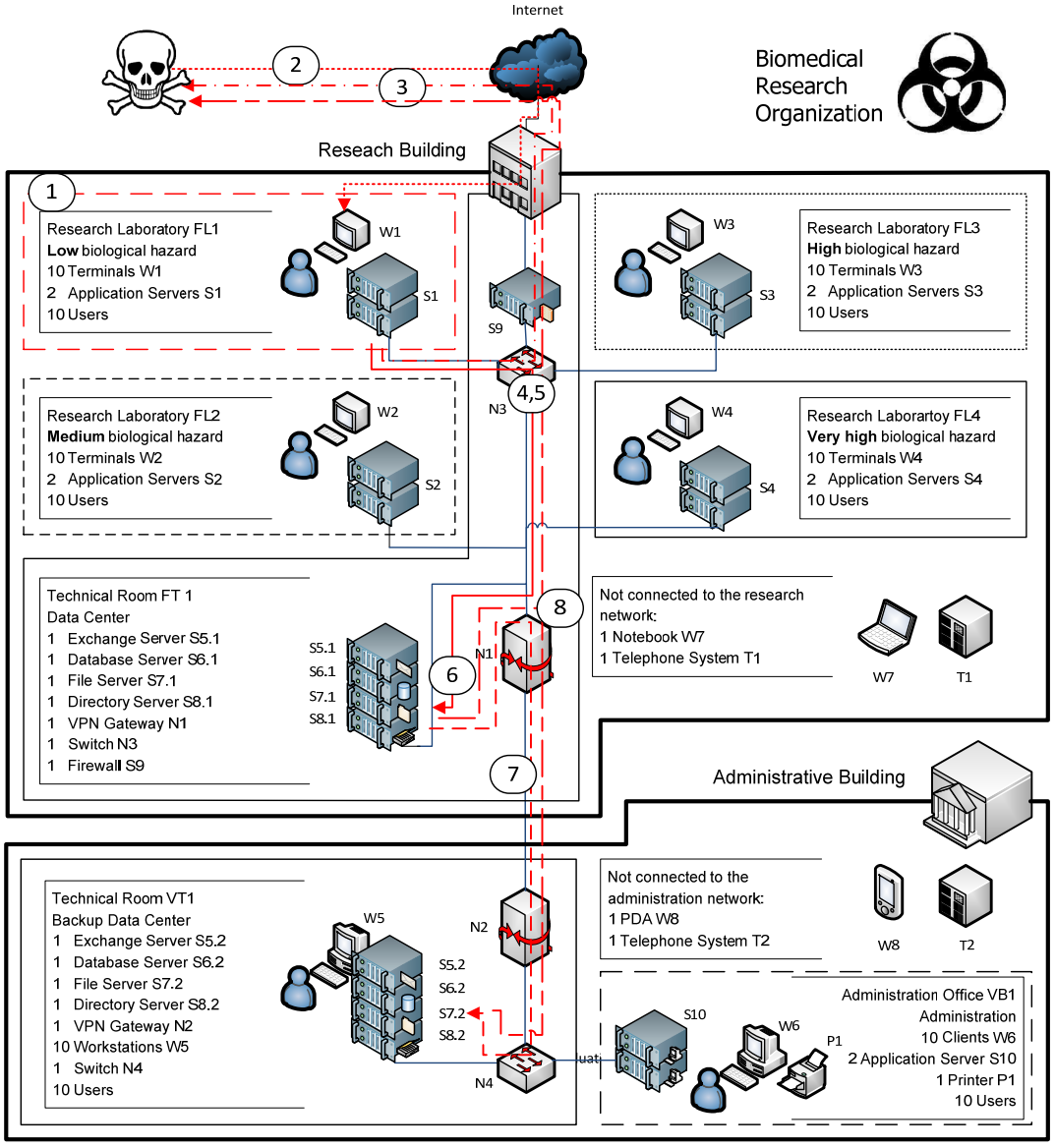

Abb. 6: Beispielszenario Organisationsdiagramm (eigene Darstellung angelehnt an [Schi14])

Mithilfe der Gefährdungsanalyse können Gefährdungskaskaden anhand der vorgegebenen Struktur analysiert werden. Der in Abbildung 1 dargestellte APT Lebenszyklus wird nun auf das vorgestellte Modell angewendet (siehe Abbildung 6).

In Schritt 1 (**Initial Recon**) versucht der Angreifer möglichst viele Informationen der Opferorganisation, insbesondere aus dem Forschungslabor 4 – jenes mit der höchsten Sicherheitsstufe – zu erhalten. Jedoch verfügen lediglich die User aus dem Forschungslabor 1 über einen vollwertigen Internetzugang und sind daher aus Sicht des Angreifers das primäre Ziel für ein Remote-Backdoor. Die Strategie lautet, an einen Anwender aus dem Forschungslabor 1 eine Spear-Phishing-Mail mit einem Absender aus dem Verwaltungsbüro 1 zu senden und so einen ersten Ansatzpunkt für weitere Aktivitäten zu erhalten. Dieser wird im vorgestellten Beispiel durch versuchtes Ansprechen eines Users (also Ausnützung des menschlichen Faktors) im Forschungslabor 1 gefunden (Abbildung 6 – 1).

Im Schritt 2 (**Initial Compromise**) wird das vorbereitete Spear Phishing Mail durch einen Anwender in der Forschungsabteilung 1 auf dem Terminal W1 geöffnet, das als Anhang enthaltene Zip-File extrahiert und ein rudimentäres Backdoor (Beachhead Backdoor) installiert (Abbildung 6 – 2). Das Backdoor verbindet sich daraufhin sofort über das Internet mit dem C2 (*Command and Control*) Server des Angreifers (Abbildung 6 – 3).

Anschließend wird im Schritt 3 (**Establish Foothold**) der Tunnel aus dem Inneren der Organisation zu einem vom Angreifer kontrollierten System dazu genutzt, um auf dem Zielsystem ein Standard-Backdoor mit mehr Möglichkeiten für den Angreifer zu installieren. Somit setzt sich der Angreifer auf dem lokalen Anwendungsserver des Labors 1, S1, fest (Abbildung 6 – 4).

Die Schrittfolge 4 startet mit der Subphase **Escalate Privileges**, um Zugriff auf mehr Ressourcen des Netzwerkes zu erhalten. Dabei werden lokale Benutzernamen und Passwörter sowie weitere Informationen über Abhören des Netzwerkverkehrs gesammelt. Dadurch erhält der Angreifer Kenntnis über die Struktur und mögliche Authentifizierungsinformationen im internen Netzwerk (**Internal Recon**) (Abbildung 6 – 5). Im Beispiel werden in der folgenden Subphase **(Move Laterally**) das lokale sowie das entfernte Rechenzentrum identifiziert, auf welchem die gewünschten Zieldaten vermutlich abgelegt sind. Ausgehend vom Anwendungsserver S1 kann der Angreifer einen Softwareschwachstellenscan am Fileserver durchführen. So kann der Angreifer aufgrund fehlender Softwarepatches den internen Fileserver S7.1 vom Anwendungsserver S1 übernehmen (Abbildung 6 – 6). Im Zuge von **Maintain Presence** werden die Spuren verwischt und dabei der Ankerpunkt auch auf den Cluster-System Fileserver S 7.2 ausgeweitet (Abbildung 6 – 7).

Auf den infiltrierten Systemen werden verdeckte Kommunikationskanäle (Covered Channels) implementiert, etwa mithilfe von verschlüsselten RAR-Files, um im Schritt 4 **(Complete Mission**) dort abgelegte streng geheime Informationen zu sammeln und unbemerkt über die zuvor etablierten Kommunikationskanäle abzutransportieren (Abbildung 6 – 8).

Die graphenorientierte Modellierung des oben beschriebenen Szenarios wird in Abbildung 7 visualisiert. Die Implementierung mit Hilfe einer Graphendatenbank erlaubt es, je nach den betrachteten Komponenten einen spezifischen Blickwinkel einzunehmen und Gefährdungskaskaden pointierter darzustellen. Durch die einfache Erweiterbarkeit der Graphendatenbank sind nachträgliche Justierungen auch leicht möglich. Die Details der Modellierung werden im Beispielsfall durch den Aufbau und die Inhalte von IT-Grundschutz geliefert. Von dort stammen die wichtigsten Systemkomponenten für die Modellierung des Anwendungsszenarios (vgl. mit Abbildung 7). Die elliptischen Formen stellen die Unternehmenswerte dar, die Pfeile deren

Abhängigkeiten (*requires*). Letztere werden im Rahmen einer Szenarioanalyse ermittelt. Damit wird die Top-Down-Risikovererbung zwischen Subsystemen festgelegt und gleichzeitig eine Vorgabe für potentielle Bottom-Up-Gefährdungs-Ketten (*gives_rise_to*) gemacht. Die Unternehmenswerte (Ellipsen) werden durch IT-Grundschutz-Bausteine (Sechsecke) beschrieben (*described_by*). Die Modellierung der Gefährdungen (Trapeze) erfolgt durch „*threatened_by*“, jene der Sicherheitsmaßnahmen (Rechtecke) durch „*mitigated_by*“-Relationen. Darauf aufbauend können für Detailanalysen die verfügbaren Gefährdungen mithilfe von „*gives_rise_to*“-Verbindungen zu Gefährdungskaskaden zusammengestellt werden. Anlehnungen für potentielle Verbindungen können aus dem Geschäftsauswirkungsmodell (*described_by*) sowie aus der Taxonomie von IT-Grundschutz (z.B. vorsätzliche Handlungen) gewonnen werden. Dieses Gefährdungskaskadenmodell adressiert die potentiellen Korrelationen nur auszugsweise, ermöglicht aber die leichte Berechnung verketteter Wahrscheinlichkeiten.

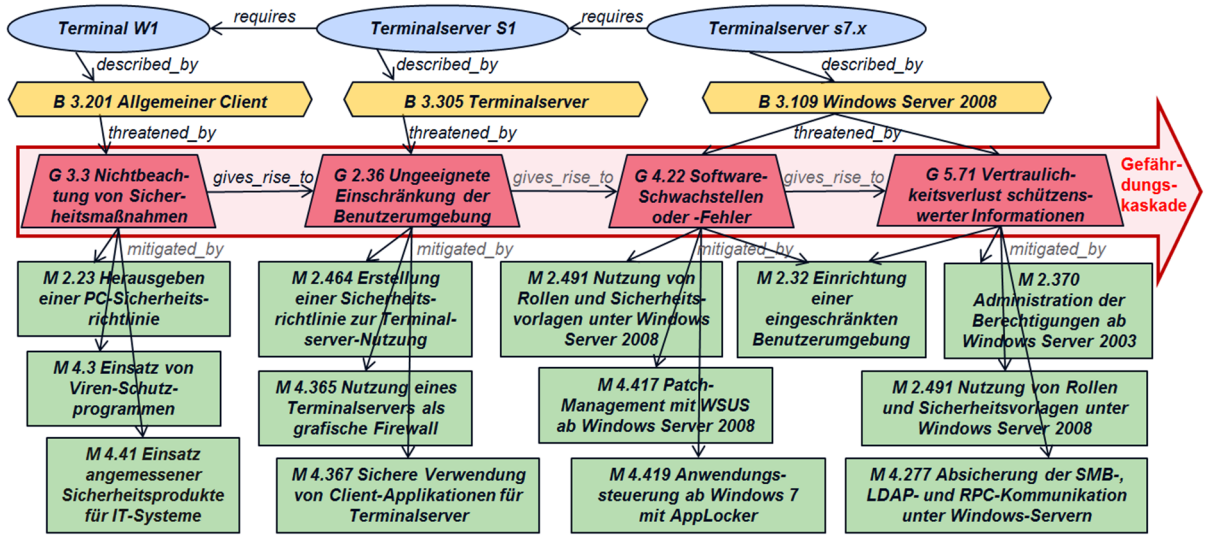

Abb. 7: Graphenbasierte Darstellung des Anwendungsszenarios (auszugsweise).

Konkret wird zu Beginn der Beispiels-APT-Attacke am Terminalsystem *W1* (*Baustein B 3.201 Allgemeiner Client*) eine Spear-Phishing-Mail geöffnet (vgl. mit Abbildung 6). Die schlagend gewordene Gefährdung *G 3.3 Nichtbeachtung von Sicherheitsmaßnahmen* aus dem BSI Grundschutz-Standard wäre durch die folgenden relevanten Maßnahmen adressiert gewesen:

- M 2.23 Herausgeben einer PC-Sicherheitsrichtlinie
- M 4.3 Einsatz von Viren-Schutzprogrammen
- M 4.41 Einsatz angemessener Sicherheitsprodukte für IT-Systeme

Anschließend wird am zugehörigen Terminalserver *S1* (*Baustein B 3.305 Terminalserver*) ein Standard-Backdoor installiert, was aufgrund der Ausnutzung der Gefährdung *G 2.36 Ungeeignete Einschränkung der Benutzerumgebung* möglich ist. Dies hätte durch die folgenden Maßnahmen verhindert werden können:

- M 2.464 Erstellung einer Sicherheitsrichtlinie zur Terminalserver-Nutzung
- M 4.365 Nutzung eines Terminalservers als grafische Firewall
- M 4.367 Sichere Verwendung von Client-Applikationen für Terminalserver

Ausgehend von Terminalserver *S1* kann ein Softwareschwachstellenscan durchgeführt werden. Mit seiner Hilfe kann der Angreifer am Fileserver *S7.1* oder später dann Fileserver *S7.2* (*Baustein 3.109 Windows Server 2008*) die Gefährdung *G 4.22 Software-Schwachstellen oder -Fehler* ausnutzen, wobei die folgenden Maßnahmen in dem Beispiel nicht greifen:

- M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung
- M 2.491 Nutzung von Rollen und Sicherheitsvorlagen unter Windows Server 2008
- M 4.417 Patch-Management mit WSUS ab Windows Server 2008
- M 4.419 Anwendungssteuerung ab Windows 7 mit AppLocker

Entsprechend wird dadurch die Folgegefährdung *G 5.71 Vertraulichkeitsverlust schützenswerter Informationen* ausgelöst, die üblicherweise von folgenden Maßnahmen adressiert wird:

- M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung
- M 2.370 Administration der Berechtigungen ab Windows Server 2003
- M 2.491 Nutzung von Rollen und Sicherheitsvorlagen unter Windows Server 2008
- M 4.277 Absicherung der SMB-, LDAP- und RPC-Kommunikation unter Windows-Servern

Die Risikovererbung zwischen den Komponenten können für quantifizierbare Analysen durch passende funktionale Beziehungen, etwa Maximum, Summe, Produkt, Minimum oder mit komplexeren normalisierten, gewichteten oder wertbegrenzten Variationen davon realisiert werden, wobei hier Weighted Weakest Link oder Prioritized Sibling denkbar erscheinen [Schi14][WaWu97]. Relevante Kennzahlen für APTs, die in quantitative Risikoberechnungen einfließen könnten, sind z.B. *Anzahl der Versuche, Zugang zu Passwortfiles zu erhalten*; *Anzahl der unautorisierten Konfigurationsänderungen*; *durchschnittliche Zeit, Clients mit unautorisierter Konfiguration zu detektieren, etc.*

5 Conclusio

In diesem Artikel wird auf Basis eines exemplarischen Falls eine Advanced-Persistent-Threat-Attacke (APT), angelehnt an den Vorfall der chinesischen Wirtschaftsspionage, wie vom US-Unternehmen Mandiant in [Mand13] beschrieben, anhand eines graphenbasierten Risikoanalyseansatzes modelliert. Dabei wird auf ein mehrstufiges Analysemodell aus [Schi14] unter Verwendung von unterschiedlichen Abstraktions- und Generalisierungsebenen aufgebaut. Ein praktisches Anwendungsbeispiel dient der Veranschaulichung.

Im Allgemeinen muss ein wirkungsvoller Ansatz zur Früherkennung von APTs gewährleisten, dass die Betrachtung der Gefahren, die von APTs ausgehen, in alle sicherheitsrelevanten Entscheidungen einfließt. Zusätzlich muss ein solcher Ansatz auf einem IKT-Risikomodell aufbauen, das eine generalisierende Überführung in ein unternehmensweites Risikomodell erlaubt und das verschiedene Eskalationsstufen zur Verfügung stellt.

Die neueren Angriffspunkte von Cyber-Kriminellen konzentrieren sich zunehmend auf den Faktor Mensch, um über diese „Schwachstelle“ im System einen ersten Zugriff auf Clientsysteme zu erhalten. Standard-konfigurierte interne Arbeitsplatzrechner, Notebooks oder andere mobile Systeme dienen dann als Hub für weitere Angriffe, indem deren Berechtigungen genutzt werden, um weitere intern erreichbare IKT-Systeme zu kompromittieren. Mögliche Methoden zur Risikoanalyse sowie entsprechende Gegenmaßnahmen müssen, um diese Form von Angriffen effektiver zu adressieren, daher den Schwerpunkt auf Schwachstellenkaskaden legen. Diese

Kaskaden stellen eine Verkettung von Angriffspunkten dar, dessen aufeinander folgende Ausnutzung zu einem relevanten Schadenspotential führt.

Im Rahmen des Artikels wurde gezeigt, dass die Verwendung einer Graphendatenbank zur Modellierung und Inferenzanalyse der Gefahrenkaskaden im Gegensatz zu einem relationalen Datenmodell einige Vorteile bringt. Hierzu gehört etwa die generische Formulierung von Statements, die es erlaubt, je nach Fokus aus dem Metaschema für jeden Objekttyp individuell die konkrete Situation abzuleiten. Somit ergibt sich jeweils ein sehr spezifischer Blickwinkel, der bei der vorliegenden Problemstellung, Gefährdungskaskaden und ihre Beziehungstypen sichtbar zu machen, optimal einsetzbar ist. Darüber hinaus ermöglicht das schemalose Datenmodell von Graphendatenbanken eine leichte Anpassbarkeit bei der Modellierung und durch den Einsatz von Traversals im Graphen können Berechnungsfunktionen ohne Adaption des Business-Codes integriert werden.

Um eine Korrektheit der Ergebnisse zu gewährleisten, muss allerdings darauf geachtet werden, dass die Umgebung, in der die Methode eingesetzt wird, weitgehend ausdefiniert ist und keinen zu hohen Grad an Ungewissheit aufweist. Zusätzlich muss der Detailgrad der Risikofaktoren in Anlehnung an die Granularität der Ergebnisse angemessenen gewählt werden, um eine einheitliche Verteilung der Risikowerte sicherzustellen.

Danksagung

Dieser Artikel wurde im Rahmen des Projekts „MetaRisk – Meta-Risiko-Modell für kritische Infrastrukturen“ erstellt, welches durch das KIRAS-Programm der österreichischen Forschungsförderungsgesellschaft (FFG) gefördert wird (Projekt-Nr. 840905).

Literatur

[Bmi13] BMI: *Polizeiliche Kriminalstatistik 2013*, Berlin (2013)

[Brew14] R. Brewer: Advanced persistent threats: minimising the damage. In: *Network Security* Bd. 2014 (2014), Nr. 4, S.5–9

[Bsi00a] BSI: *IT-Grundschutz-Standards*. URL https://www.bsi.bund.de/DE/Publikationen/BSI_Standard/it_grundschutzstandards.html. - abgerufen am 2015-03-19

[Bsi00b] BSI: *IT-Grundschutz-Kataloge*. URL https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/kataloge.html. - abgerufen am 2015-03-19

[Cole00] T.W. Coleman: *Cybersecurity Threats Include Employees*. URL http://www.internationalpolicydigest.org/2014/05/12/cybersecurity-threats-include-employees/. - abgerufen am 2015-03-19. — International Policy Digest

[Comm13] The Commission on the Theft of American Intellectual Property: *The IP Commission Report*: National Bureau of Asian Research, (2013)

[FSSF15] I. Friedberg, F. Skopik, G. Settanni, R. Fiedler: Combating advanced persistent threats: From network event correlation to incident detection. In: *Computers & Security* Bd. 48 (2015), S. 35–57

[GöKM15] J. Göllner, J. Klerx, K. Mak: *Wissensmanagement im ÖBH: Foresight in der strategischen Langfristplanung*, *Schriftenreihe der Landesverteidigungsakademie*. Bd. 5/2015. Vienna, Austria (2015)

[GöKW10] J. Göllner, M. Klaus, R. Woitsch: *Grundlagen zum Wissensmanagement im ÖBH: Teil 2: Wissensbilanz als Steuerungsinstrument im ÖBH: Ein Evaluierungs-Rahmenwerk aus der Sicht praktischer Anwendungen*, *Schriftenreihe der Landesverteidigungsakademie*. Vienna, Austria (2010)

[Gree14] G. Greenwald: *Die globale Überwachung: der Fall Snowden, die amerikanischen Geheimdienste und die Folgen*. München: Droemer Knaur, (2014)

[Inte13] Internet Crime Complaint Center: *2013 Internet Crime Report*: Federal Bureau of Investigation, (2013)

[Isoi11] ISO/IEC 27005:2011: *Informationssicherheits-Risikomanagement* (2011)

[Mand13] Mandiant Intelligence Center: *APT1. Exposing One of China's Cyber Espionage Units*. Alexandria, Washington, DC: Mandiant, (2013)

[MILP14] D. Moon, H. Im, J. Lee, J. Park: MLDS: Multi-Layer Defense System for Preventing Advanced Persistent Threats. In: *Symmetry* Bd. 6 (2014), Nr. 4, S. 997–1010

[Neoj00] Neo4j Graph Database: *Intro to Cypher - Neo4j Graph Database*. http://neo4j.com/developer/cypher-query-language/. - abgerufen am 2015-03-25

[Pone14] Ponemon Institute: *Exposing the Cybersecurity Cracks: A Global Perspective Part 2: Roadblocks, Refresh and Raising the Human Security IQ*. Traverse City, Michigan, USA, (2014)

[Sans00] SANS Institute: *Critical Security Controls: Guidelines*. http://www.sans.org/critical-security-controls/guidelines.

[Schi14] S. Schiebeck: *An Approach to Continuous Information Security Risk Assessment focused on Security Measurements*. Wien, University of Vienna, Dissertation, (2014)

[Tank11] C. Tankard: Advanced Persistent threats and how to monitor and deter them. In: *Network Security* Bd. 2011 (2011), Nr. 8, S. 16–19

[UrMy15] R.-G. Urma, A. Mycroft: Source-code queries with graph databases—with application to programming language usage and evolution. In: *Science of Computer Programming* Bd. 97 (2015), S. 127–134

[WaWu97] C. Wang, W.A. Wulf: Towards a Framework for Security Measurement. In: *Proc. of 20th National Information Systems Security Conference*. Baltimore, Maryland, (1997)

[WoMG10] R. Woitsch, K. Mak, J. Göllner: *Grundlagen zum Wissensmanagement im ÖBH: Teil 1: Ein WM-Rahmenwerk aus der Sicht praktischer Anwendungen*, *Schriftenreihe der Landesverteidigungsakademie*. Vienna, Austria, (2010) — ISBN 978-3-902670-13-7