Sicherheit von komplexen Systemen

Dr. Ulrich Kampffmeyer

PROJECT CONSULT
Unternehmensberatung
Dr. Ulrich Kampffmeyer GmbH

Hamburg, Dezember 2020

Sicherheit von komplexen Systemen

IT-Systeme werden immer komplexer. Die Administration, Kontrolle und Sicherung dieser Systeme wird immer schwieriger. Gerade die Vernetzung solcher komplexer Systeme über das Internet macht die Systeme noch anfälliger gegen Einbrüche und den Mißbrauch von Daten. Immer wieder liest man von “gestohlenen” (die Daten sind vielfach noch da, wurden aber illegal kopiert und verbreitet) Datensätzen mit E-Mails und geknackten Passworten. Passwortmanager-Software gibt immer häufiger länger werdende Listen von kompromittierten Passworten auch bekannter, großer Webseiten aus. Nachrichten über gigantische Hacks, wie aktuell im Dezember 2020 öffentlich in den USA bekannt wurde, zeigen die Möglichkeiten des Cyberwars ansatzweise auf. Neben den anvisierten Regierungsstellen in den USA waren auch Zigtausende andere Systeme über Monate für die Hacker offen. Die Manipulation von technischen Komponenten in Atomkraftwerken im Iran zeigten schon vor längerem, wie wenig Sicherheit technisch gegen gewiefte Hacker gegeben ist. Und aktuell wird dies noch durch den IOT-Boom mit häufig per-se unsicheren vernetzten und steuerbaren Komponenten weiter befördert.

Wie steht es also um die Sicherheit in komplexen IT- und Softwaresystemen?

Wir möchten hier zwei Hypothesen gegeneinander in den Raum stellen.

Hypothese 1:
Komplexe IT- und Softwaresysteme sind nicht mehr technisch sicherbar, nur noch organisatorische Maßnahmen und verantwortliches Handeln helfen

Die Administration und Kontrolle komplexer IT- und Software-Umgebungen ist kaum noch möglich. Dies wird auch durch automatische Updates von Software, die vielfach wenig nachvollziehbar Parameter und Eigenschaften verändern, erschwert. Besonders wenn häufiger Aktualisierungen eingespielt werden, die natürlich die Abhängigkeiten mit anderen Komponenten, Systemen und Programmen nicht abdecken können, wird die Lage schnell unüberschaubar. Selbst professionelle Teams in Rechenzentren stoßen hier zunehmend an ihre Grenzen, wenn hunderte von Modulen, Programmen, Schnittstellen und Abhängigkeiten gehandhabt werden müssen. Der Schutz von Missbrauch von Informationen durch interne Mitarbeiter wie auch durch Einbrüche von außen, lässt sich nur noch unzureichend sicherstellen. Die Auswertung von Protokollen und Logs steht meistens vor einem nicht verwertbaren Datengrab.

So wird hier häufig auf die Verantwortung der Mitarbeiter gesetzt. Es gilt mehr Sorgfalt bei der Nutzung externer Quellen (Webseiten mit Schadcode) und eingehender Nachrichten (E-Mail mit Schadcode) anzutrainieren und die Risiken bewusster zu machen. Es gilt das Bewusstsein zu schärfen, dass man keine vertraulichen Daten des Unternehmens auf Notebooks oder Sticks kopiert durch die Gegend trägt und vertrauliche Information nicht in ungesicherte, private Cloud-Speicher kopiert. Noch immer wird mit Passworten und der Versendung von Information zu lax umgegangen. Es gilt ein Verantwortungsbewusstsein und eine Loyalität mit dem Arbeitgeber zu erzeugen, die einen verantwortungsvollen Umgang mit Informationen fördert und Missbrauch verhindert (auch wenn dies gerade in Corona-Zeiten mit Heimarbeit besondere Herausforderungen darstellt). Verantwortliches Umgehen mit Unternehmensinformation gehört zur Stärkung solcher Initiativen auch belohnt.

Aber auch das Unternehmen muss hier aktiv werden und Information nach Wert, Vertraulichkeit, Rechtscharakter und Sicherheit klassifizieren. Solche als Records eingestufte Informationen gehören in besonders gesicherte Systeme, die auch die unkontrollierte Redundanz verhindern.

Alle diese Maßnahmen orientieren sich an den MitarbeiterInnen und deren Verhalten. Die “Haupteinbruchspforte Mensch” in die Systeme soll geschlossen werden. Zusammengefasst soll in dieser Hypothese der “Human Factor as Solution for Information Security Management” im Zentrum von Sicherheits- und Schutzmaßnahmen stehen.

Hypothese 2:
Künstliche Intelligenz übernimmt die Sicherung von IT- und Softwaresystemen

Das Thema Automatisierung steht bei der Sicherung komplexer IT- und Softwaresysteme hoch im Kurs. Das Arbeiten mit Vererbung von Eigenschaften auf Basis von Klassen hilft den Überblick zu bewahren. Jedoch sind hier in hybriden, heterogenen und komplexen Systemen Grenzen gesetzt. Administrationswerkzeuge werden zwar durch Analytics, Vererbung und Automatisierung von Verwaltungsprozessen einfacher und fehlerfreier handhabbar, aber auch für Menschen intransparenter. Man setzt nun auf Künstliche Intelligenz (KI) und Maschinenlernen (ML) um das Problem der Verwaltung und Kontrolle solcher Systeme zu überwinden. Da KI Künstliche Intelligenz inzwischen sich ohne menschliche Eingriffe selbst programmiert, optimiert und repliziert, ist eine Kontrolle und Beherrschung durch den Menschen sowieso kaum noch gegeben. Nimmt man nun die Hypothese 2 “Artificial Intelligence as Solution for Information Management Security” lassen sich drei verschiedene Anwendungsbereiche lokalisieren, wo KI bereits zum Einsatz kommt:

(1) Automatisierung der Administration
Mit geeigneten Algorithmen, vordefinierten Klassen, selbstlernenden Komponenten und nachvollziehbaren Workflows übernimmt die KI bereits Aufgaben der Einrichtung neuer und Entfernung ausscheidender Benutzer, Überwachung der Kompatibilität von Schnittstellen und Komponenten bei Updates und “Predictive Maintenance” sowie Vormeldung von wahrscheinlich auftretenden Problemen. Ziel ist Vereinfachung, Beschleunigung und Konsistenz-Schaffung in den komplexen vernetzten Systemen. Maschinenlernen steht hier noch am Anfang.

(2) Klassifikation von Information
Mit Analytics, vordefinierten Taxonomien und Ontologien und Maschinenlernen können die wichtigen, vertraulich zu haltenden Informationen selbst aus den weniger geschützten Systemen ermittelt und in sicherere Systeme mit höherem Schutz migriert werden. Dabei werden auch Caches, Zwischenversionen, lokale Kopien etc. ermittelt und systematisch gesäubert. Man gewinnt hierdurch die Kontrolle über die Inhalte und deren Nutzung selbst – ein Thema der Information Governance. Durch die Verwendung nur einmal beschreibbarer Speicherbereiche und zusätzlicher Offline-Sicherungsspeicher lässt sich die Information auch gegen Veränderung und Löschung schützen, so dass zumindest Manipulation und Verlust bei Einbrüchen in Systeme verhindert werden kann.

(3) Auswertung von Kommunikation, Transaktionen und Protokollen
Gerade angesichts der Informationsflut kann Künstliche Intelligenz mit Mustererkennung und Analytics genutzt werden, um aktuell oder zumindest zeitnah Einbrüche und Missbrauch festzustellen. Zusammen mit einer effizienten Sicherungsstrategie für die Daten kann so häufig rechtzeitig ein Zustand wie vor dem Einbruch wiederhergestellt und z.B. Schadsoftware lokalisiert und entfernt werden. Dies beginnt bei IOT-Transaktionen, führt über Hintergrundsoperationen und administrative Aktivitäten bis zum Standard-Anwendungsgebiet

E-Mail- und Web-Browsing-Kontrolle. Aus “Fraud Detection” kann durch Maschinenlernen auch automatisierte “Fraud Prevention” werden.

Eines darf man bei allen drei Szenarien für den KI-Einsatz nicht vergessen: Wissen über die vorhandene Information und die Prozesse nebst Ordnung und Nachvollziehbarkeit hilft enorm auch selbstlernenden Systemen. Der Ansatz der Hypothese 2 “Artificial Intelligence as Solution for Information Management Security” lässt den Menschen weitgehend außen vor und setzt auf die Geschwindigkeit, die Stringenz von Algorithmen, die auch mit großen Datenmengen und vernetzten Systemen besser als die Auffassungsgabe und Disziplin des Menschen klar kommen.

Braucht man beide Ansätze?

Ja, aber aus verschiedenen Gründen.
Hypothese 1 “Human Factor” wird immer wichtiger, um den Menschen mit seiner Arbeitswelt zu versöhnen, ihm Identifikation und Sinn bei seiner Arbeit zu geben und ihm die Angst vor dem Software-Roboter zu nehmen. Sicherheit wird hier eine zukünftig nachgeordneter Rolle spielen, auch wenn das Home-Office hier einige technische Schwierigkeiten und gerade in Bezug auf Sicherheit offene Flanken bietet. Generell Bewusstsein für den Umgang mit Information, dem Schutz vertraulicher Information, zu schaffen, ist immer eine notwendige Voraussetzung, um Durchgängigkeit und Nachhaltigkeit beim Thema Sicherheit zu schaffen.
Hypothese 2 “Artificial Intelligence” ist wahrscheinlich die einzige Chance das immens schnell und wenig kontrollierte Wachstum der komplexen, vernetzten Systeme in den Griff zu bekommen. Je einfacher sich ein System dem Menschen zeigt und durch ihn nutzbar ist, je höher ist in der Regel die hinter den Oberflächen versteckte Komplexität. Durch verbundene Services und Micro-Services in einer global vernetzten Welt sind wir angesichts der Datenmengen im Yotta-Byte-Bereich und der milliardenfachen Verquickungen von Komponenten und Geräten bereits jenseits der Möglichkeiten, dies noch durch Menschen administrieren und kontrollieren zu lassen. Systeme, regelbasiert, selbstlernend, sich selbst erfindend, werden hier die einzige Chance sein.
In dem Maße, wie Angriffe und Einbrüche immer intelligenter, schwieriger aufzudecken und zu beheben sind, müssen Administration und Schutz der Systeme ständig nachgezogen, besser noch, vorausschauend sicherer gemacht werden. Während Regierungen und große Unternehmen dies noch aus eigener Kraft – meistens – können, sind alle anderen auf vertrauenswürdige Cloud- und On-Premises-Software-Anbieter angewiesen. Aber auch diese Anbieter werden immer häufiger durch Dritte unwissentlich oder gar selbst als “Einbrecher”, “Hacker” und “Hehler” tätig. Das Thema Informations- und Systemsicherheit wird nicht nur in 2021 ein herausragendes Thema sein, sondern für die kommenden Jahrzehnte Entwicklung von Lösungen, Fragen der Ethik und Vertrauenswürdigkeit sowie Diskussionen um Sicherheit und Schutz bestimmen.

Produktabwahl versus Produktauswahl

Über den Autor

Dr. Ulrich Kampffmeyer ist seit über 35 Jahren im Thema Informationsmanagement zu Hause. Als Geschäftsführer und Unternehmensberater seines Beratungsunternehmens PROJECT CONSULT (http://PROJECT-CONSULT.de) berät er Unternehmen bei der Strategie, Konzeption, Einführung, Ausbau und Migration von Information Management-Lösungen.
Er gründete und leitete Fachverbände, arbeitete bei internationalen Standardisierungen mit und gilt als Mentor der Information-Management-Branche in Europa.
Dr. Kampffmeyer ist international anerkannter Autor, Kongressleiter, Referent und Moderator zu Themen wie Information Management, Information Governance, elektronische Archivierung, Records Management, ECM Enterprise Content Management, Dokumentenmanagement, Workflow, Rechtsfragen, Wissensmanagement, Digitalisierung und
Collaboration. Auf zahlreichen nationalen und internationalen Kongressen und Konferenzen wirkte er als Keynote-Sprecher mit. Er engagiert sich besonders für die Rolle und Ausbildung des Information Professional der Zukunft.
Von Fachzeitschriften wurde zweimal unter die 100 wichtigsten IT Macher Deutschlands gewählt. Sein Curriculum Vitae findet sich auf Wikipedia http://bit.ly/WP_DrUKff

PROJECT CONSULT

Die PROJECT CONSULT GmbH ist ein hersteller- und produktunabhängiges Beratungsunternehmen für Information Management und Information Governance.
Zum Beratungsportfolio gehören IT-Strategie, Fachberatung, Planung und Organisation zu Einführung, Migration und Abnahme von Informationssystemen; Projektmanagement, Change Management und Coaching für Projekte des Informationsmanagement wie elektronische Archivierung, Knowledge-, Dokumenten-, E-Mail-, Enterprise-Content-Management und Compliance.

Impressum

ISSN 1349-0809, Creative Commons CC by-nc-nd 4.0 Open Access.

Links. Angegebene URL waren zum Erscheinungszeitpunkt gültig. Die Inhalte referenzierter Webseiten liegen ausschließlich in der Verantwortung des jeweiligen Betreibers.

PROJECT CONSULT Impressum und AGB: Impressum

Geschäftsleitung und V. i. S. d. P.: Dr. Ulrich Kampffmeyer
Anschrift der Redaktion:
PROJECT CONSULT Unternehmensberatung
Dr. Ulrich Kampffmeyer GmbH
Isestraße 63, 20149 Hamburg
Telefon: +49 40 412856 53
E-Mail: presse@project-consult.com
http://www.project-consult.de