KI-gestützte Cybersicherheit: Wie Mensch und Maschine sich intelligent verhalten

Autor: Arnold Krille, genua GmbH

Wenn KI und Cybersicherheit in einem Satz genannt werden, sollte speziell auf der Seite der Verteidiger genau zwischen Hype und tatsächlich wirksamen Methoden unterschieden werden. Gemeinsam mit ihren Forschungspartnern erforscht die genua GmbH im BMBF-geförderten Forschungsprojekt „Wintermute“ (https://www.projekt-wintermute.de) Möglichkeiten, wie IT-Administratoren mittels verschiedener KI-Methoden realistisch unterstützt werden können, um die IT-Sicherheit in Organisationen zu erhöhen.

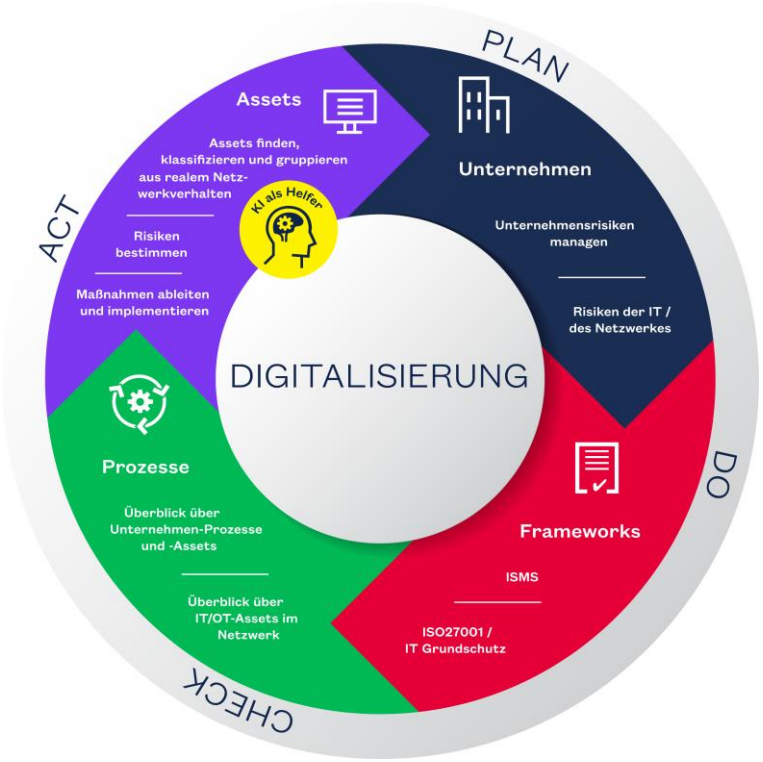

Schaubild 1: KI-gestütztes Vorgehensmodell für das IT- und Informationssicherheitsmanagement. Die KI als „Helfer“ erlaubt die Integration von Unternehmenssicht und Realität im Netzwerk.

Cybersicherheit in Unternehmen

Keine Organisation betreibt den Aufwand der IT zum Selbstzweck. Die Digitalisierung der Geschäftsprozesse und damit der Wertschöpfung wird durch „die IT“ bereitgestellt und ermöglicht. Die Ziele der IT sind damit die Ziele des Unternehmens. Die Risiken des Unternehmens sind damit allerdings auch stark von den Risiken der IT beeinflusst.

Speziell der Ressourcenmangel in der IT, insbesonders in der IT-Sicherheit, macht dabei vielen Unternehmen zu schaffen. Generell fehlt es an Personen und Wissen, um den Herausforderungen der Zeit gut gewappnet zu begegnen.

Herausforderungen für die IT

Die Computernetzwerke der IT dienen dazu, die Geschäftsprozesse der Organisationen zu stützen. Die Komplexität der heutigen Geschäftsprozesse schlägt sich damit in der Komplexität der IT-Systeme und Netzwerke nieder. Damit wird es für System- und Netzwerkadministratoren immer schwerer, den Überblick zu behalten – häufig ist dieser verloren gegangen. Auch für neue Kollegen oder Consultants, die für eine kurze Zeit unterstützen sollen, ist es fast unmöglich, sich kurzfristig Überblick über ein Netzwerk zu verschaffen. Damit ist aber auch der Überblick über die Risiken nicht mehr gegeben; ein Zustand, der für verantwortungsvoll geführte Unternehmen nicht haltbar ist.

Um wirksame Maßnahmen der Risikominimierung zu betreiben, braucht es einen Überblick über die Prozesse und Assets eines Unternehmens, in der IT also über das Netzwerk und seine Geräte. Nur wer die eigenen Assets kennt, kann passende Maßnahmen der Strukturierung und Risikominimierung einführen und auf ihre Wirksamkeit hin prüfen. Und nur wenn der Administrator den Überblick über die real vorhandenen Assets hat, kann er Abweichungen zwischen dem Soll-Zustand und realem Ist-Zustand erkennen und angemessen handeln. Solche Abweichungen können viele Ursachen haben, von historisch gewachsenen Zuständen über Fehlkonfigurationen bis hin zu bewussten Angriffen durch Dritte.

Das ISMS und die tägliche Arbeit des Administrators

Frameworks wie ein Informationssicherheitsmanagementsystem (ISMS) nach ISO27001 oder der IT-Grundschutz bieten den geeigneten Rahmen für ein strukturiertes Vorgehen zur Erfassung, Einschätzung und Behandlung von Risiken und notwendiger Maßnahmen. Der Netzwerkadministrator steht dabei vor der

Herausforderung, dass er die theoretischen Vorgaben des ISMS im realen Netzwerk umsetzen muss. Dafür sind die real existierenden Geräte (Assets) im Netzwerk zu finden und zu bestimmen. KI-gestützte Werkzeuge (z.B. cognitix Threat Defender) unterstützen den Menschen an dieser Stelle mit einer Analyse des Netzwerkverkehrs und der Erkennung der Assets. Die Kommunikationspfade im Netzwerk und das Kommunikationsverhalten liefern Informationen über die Art und Funktion der vorhandenen Geräte, sodass eine Klassifizierung stattfinden kann. Als Basis für eine einheitliche Klassifizierung dient das Schema des IT-Grundschutz. Bei der Klassifizierung können überraschende Erkenntnisse zu Tage treten, wenn beispielsweise die Smart-TVs in Meetingräumen richtigerweise als Webserver erkannt werden. Bei der Klassifizierung von Geräten hilft KI in Form von Expertensystemen.

Zur einfacheren Handhabung können im nächsten Schritt die Assets gleicher Klassifizierung gruppiert werden, um sie bei organisatorischen und technischen Maßnahmen gebündelt zu behandeln. Weiterhin hilft es dem Administrator, wenn die Komplexität des Netzwerkes vereinfacht wird oder zumindest eine vereinfachte Darstellung gefunden wird.

Für die „High Value Assets“, also die für das Unternehmen kritischen Prozesse und Systeme, ist eine individuelle Betrachtung einzelner Systeme oder sich gleich verhaltender Gruppen notwendig. Die weniger kritischen Systeme können häufig zu weicheren Clustern von ähnlichem Verhalten und ähnlichen Anforderungen des ISMS zusammengefasst werden. Bei diesem Clustering helfen KI-Methoden des Machine Learnings. Da für dieses Clustering neben dem Verhalten der Assets die Klassifizierung nach IT-Grundschutz als Ausgangsbasis genutzt wird, ermöglicht dies erklärbare, nachvollziehbare Cluster. Das KI-System kann damit für den Administrator nachvollziehbar darstellen, warum ein Asset Teil eines Cluster ist. Auch lässt sich erklären, welche Änderung im Verhalten eines Assets dafür gesorgt hat, dass es nicht mehr einem bestimmten Cluster und eventuell einem anderen Cluster zugeordnet wurde. Mit diesen Informationen erhält der Administrator den notwendigen Kontext, um zu entscheiden, ob diese Änderung eine Anomalie durch einen Angriff darstellt oder eine durch eine Maßnahme ausgelöste erwartete Änderung darstellt.

Die Inventarisierung und Klassifizierung sowie die Gruppen und Cluster erlauben es, das Risiko von individuellen Assets, Gruppen und Asset-Clustern anhand des real im Netzwerk vorhandenen Verhaltens der Geräte und der auftretenden

Verdachtsmomente zu messen – aber auch das der gesamten Infrastruktur einer Organisation, und damit eine Grundlage für die Risikobetrachtung und die Bestimmung der Security-Posture eines Unternehmens zu liefern.

Fazit

Mit dem in Schaubild 1 beschriebenen Vorgehensmodell gehen die tägliche Arbeit des Netzwerkadministrators, des Security-Experten und des ISMS Hand in Hand. Die Sicht des Unternehmens auf seine digitalen Prozesse und die damit verbundenen Risiken werden mit der realen Situation des Netzwerks verknüpft. Für den Administrator reduziert sich der Aufwand im Rahmen der Compliance-Vorgaben. Und für das Risikomanagement des Unternehmens ist sichergestellt, dass die dokumentierte Situation der Realität entspricht.