Gefährdung und Absicherungen von IT-Infrastrukturen: Anomalie-Erkennung durch unterschiedliche Sicherheitssysteme

Der Stand der IT-Sicherheitstechnik in den Verwaltungen und Unternehmen erstreckt sich heute von Firewalls über Proxys bis hin zu Anti-Viren-Systemen. Dabei steht meistens die Verfügbarkeit der Betriebsprozesse im Vordergrund und nicht die Analyse der IT-Sicherheit.

Text: Prof. Dr.-Ing. Kai-Oliver Detken / Bilder: Autor und AdobeStock
AdobeStock_114915621 von peterschreiber.media, AdobeStock_200203837 von sdecoret

Neuere Lösungen wie Network Access Control (NAC), Intrusion Detection System (IDS) oder Security Information and Event Management (SIEM) sucht man daher vergeblich. Dabei drängen inzwischen weitere Sicherheitslösungen, wie Endpoint Detection and Response (EDR), Extended Detection and Response (XDR) oder Security Orchestration Automation and Response (SOAR), auf den Markt. An dieser Stelle soll daher mehr Klarheit der unterschiedlichen Begrifflichkeiten geschaffen und aufgezeigt werden, woran es momentan noch hapert.

Cyber-Attacken auf Kommunen und Unternehmensnetze

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beobachtet die Gefährdungslage der IT-Sicherheit kontinuierlich und bringt dazu jedes Jahr einen entsprechenden Bericht heraus. Auch im Jahr 2020 konnte dabei eine Fortsetzung des Trends beobachtet werden, dass Angreifer Schadprogramme für cyberkriminelle Massenangriffe auf Privatpersonen, Unternehmen und andere Institutionen (wie Kommunen) nutzen. Auch das Abgreifen personenbezogener Daten sowie kritische Schwachstellen in Soft- und Hardware-Produkten konnten festgestellt werden (siehe Abbildung 1).

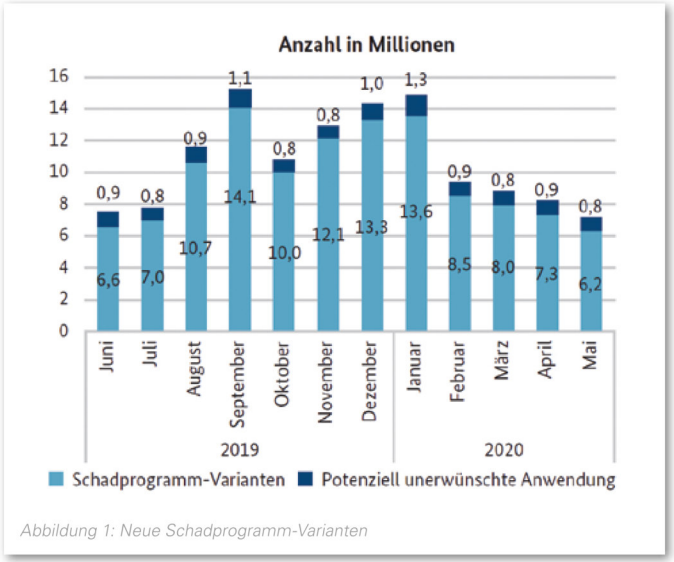

Abbildung 1: Neue Schadprogramm-Varianten

Neue Schadprogramm-Varianten

Zu den Schadprogrammen zählen dabei alle Computerprogramme, die schädliche Operationen ausführen oder andere Programme dazu befähigen können. Sie gelangen normalerweise über E-Mail-Anhänge oder Links auf einen Computer. Wenn der Nutzer beispielsweise auf solch einen Link klickt, wird im Hintergrund ein Schadprogramm installiert. Zusätzlich zählen unbemerkte Downloads und Maleware-infizierte Erweiterungen von normalen Programmen zu den typischen Angriffsvektoren. Für die Infektion nutzen Schadprogramme in der Regel Schwachstellen aus. Schadprogramme, die sich als gutartige Software tarnen oder in legitimen Dateien verstecken, werden als Trojaner bezeichnet und solche, die zum Beispiel mit Hilfe von Command-and-Control-Servern fernsteuerbar sind, als Bot. Als Ransomware werden Schadprogramme bezeichnet, die durch Verschlüsselung den Zugang zu Daten oder Systemen einschränken, um anschließend ein Lösegeld zu erpressen. Seit September 2019 traten neue Varianten der Schadsoftware Emotet auf, die verstärkt für Cyber-Angriffe verwendet wurden. Das Auftreten von Emotet markiert einen Methodenwechsel der Angreifer. Waren früher noch ungezielte Massenangriffe auf zufällig getroffene Ziele das Mittel der Wahl, so werden Schadsoftware-Angriffe mittlerweile immer intelligenter und – durch einen geschickt kombinierten Einsatz verschiedener Schadprogramme – gezielter. Diese vielfältigen Schadfunktionen bieten den Angreifern zahlreiche neue und fortschrittliche Angriffsvektoren, was als Advanced Persistent Threats (APT) bezeichnet wird. APTs sind daher oft langfristig geplante Angriffe auf herausgehobene Ziele, die nicht durch einfache Angriffsmuster erkannt werden können.

(Quelle: BSI-Auswertung von Rohdaten des Instituts AV-Test GmbH [1])

Verwirrende Technologie-Vielfalt

Angriffe kommen heute nicht mehr ausschließlich von außen, sondern werden in großem Maße von innen (absichtlich oder unabsichtlich) ausgeführt [2]. Hier bieten typische Sicherheitslösungen wie z.B. UTM-Firewalls oder AV-Systeme keinen alleinigen Schutz mehr an. Um interne Netz- und Serverzugriffe wirksam schützen zu können, sind daher neue Systeme entwickelt worden, die nachfolgend kurz erläutert werden. IDS/IPS-Systeme versuchen das interne Netzverhalten zu analysieren, Angriffe durch Muster zu erkennen und ggf. automatisierte Gegenmaßnahmen einzuleiten. Hier unterscheidet man zwischen host- und netzbasierten IDS-Lösungen, die auch in Kombination eingesetzt werden können. Das hostbasierte IDS schützt das Betriebssystem eines Server- oder Client-Rechners und analysiert Log- und Kernel-Daten sowie andere Systemdaten, wie z.B. Datenbanken. Das netzbasierte IDS zeichnet hingegen den Netzwerkverkehr auf und gibt Alarm bei verdächtigen Aktivitäten. Es wird versucht, ein Angriffsmuster zu erkennen und dieses mit den bekannten Mustern abzugleichen. Hybride Systeme kombinieren beide Arten miteinander, haben aber dadurch eine hohe Datenflut zur Folge, die den IT-Administrator oftmals überfordert. Daher konnten sich solche Systeme nicht am Markt durchsetzen. Um sich gegen Viren, Würmer und nicht autorisierte Zugriffe auf Serversysteme zu schützen, kann ebenfalls eine sog. Zugangskontrolle (Network Access Control, NAC) eingeführt werden. Der NAC-Ansatz ist auf die Endgeräte fokussiert und kontrolliert diese während

des Anmeldungsprozesses auf Richtlinienkonformität. Ein typisches Szenario ist es, wenn bei der Authentisierung die Aktualität des Virenscanners bzw. seiner musterbasierten Datenbank abgefragt wird. Ist diese auf dem neusten Stand, wird entsprechend der Nutzerrichtlinie der Zugriff gewährt. Ist hingegen der Virenscanner veraltet, wird das Endgerät in die Quarantänezone geschoben. Dort hat es nur Zugriff auf das öffentliche Internet sowie den Update-Server. Ist das Endgerät wieder auf einem Sicherheitsstand, der den Sicherheitsrichtlinien entspricht, kann er auf das Unternehmensnetz wie gewohnt zugreifen. Die erforderlichen Funktionen verteilen sich auf verschiedene Netzwerkkomponenten wie Router, WLAN-APs und Switches oder entsprechende Appliances, die gebündelt die Funktionalität anbieten. Falsches Nutzerverhalten und Angriffe auf Applikationsebene können allerdings nicht erkannt werden.

SIEM-Systemaufbau und Kommunikationsschnittstellen

Security Information and Event Management (SIEM) ermöglicht die Echtzeitanalyse von Sicherheitsalarmen, die von Netzwerk-Komponenten oder Anwendungen generiert werden (siehe Abbildung 2). Es können zusammenhängende Reports (Berichte) erstellt werden, die man auch für Compliance-Zwecke verwenden kann. Eine Kombination mit NAC-Systemen ist dabei durchaus erwünscht, da sich beide Sicherheitssysteme gegenseitig ergänzen können [3]. SIEM-Lösungen sammeln relevante Protokoll-, Log- und Ereignisdaten aus verschiedensten Quellen (z.B. Firewalls, IDS-/IPS-Systeme, Anti-Malware-Software oder Web-Content-Gateways). Die aus diesen Quellen aggregierten Daten werden dann von der SIEM-Lösung analysiert, um etwaige Sicherheitsprobleme übergreifend zu erkennen. SIEM ordnet die Ereignisse dabei hinsichtlich ihrer Bedeutung ein. Security-Admins obliegt anschließend die Aufgabe, die verschiedenen Ereignisse durchzusehen, um die Quelle der Bedrohung aufzuspüren [4]. Security Orchestration Automation and Response (SOAR) korreliert ähnlich wie SIEM ebenfalls Sicherheitsdaten aus verschiedenen Quellen. Während SIEM-Lösungen aber in erster Linie Protokoll- und Ereignisdaten aus der Sicherheitslandschaft innerhalb und außerhalb des Unternehmensnetzwerks zu erhalten. Mit Hilfe von SOAR werden daher auch die jeweils notwendigen Arbeitsabläufe als Reaktion auf bestimmte Sicherheitsvorfälle automatisiert. SOAR unterstützt die IT-Abteilung somit nicht nur bei der Analyse von Sicherheitsmeldungen, sondern kann auch aktiv auf Situationen reagieren. Zusätzlich versuchen Hersteller die Kommunikationsendpunkte durch Endpoint-Protection-Lösungen besser abzusichern. Für gezielte Attacken auf bestimmte Rechnersysteme ist daher Endpoint Detection and Response (EDR) entwickelt worden. Diese Systeme bieten präventiven Bedrohungsschutz, intelligente Analysen durch maschinelles Lernen und koordinierte Abwehrprozesse. Das Rechner-Betriebssystem wird nicht nur geschützt, sondern auch seine Schnittstellen (z.B. USB). Als Weiterentwicklung von EDR wird hingegen Extended Detection and Response (XDR) gehandelt. XDR kombiniert Daten aus verschiedenen Quellen, wie zum Beispiel den Endpoints, dem Netz, der Cloud und Log-Daten, mit allgemeinen Bedrohungsinformationen. Das heißt, es werden lokale Bedrohungsdaten mit externen Datenquellen kombiniert. Dadurch soll ähnlich wie bei SOAR ein vollständigeres Angriffsbild geschaffen werden.

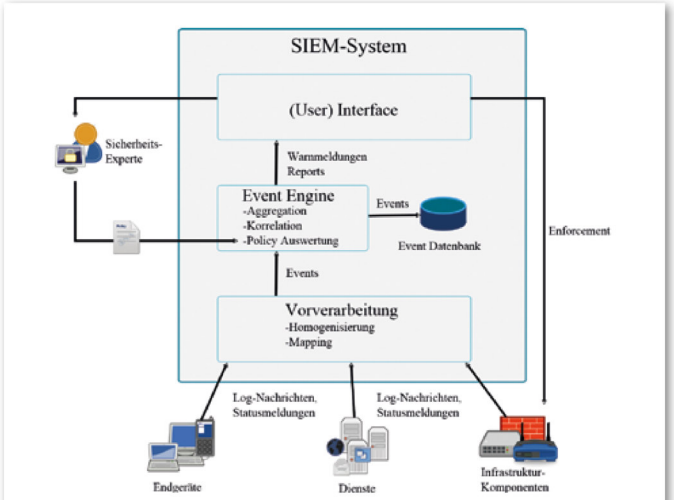

Abbildung 2: SIEM-Systemaufbau und Kommunikationsschnittstellen

traditionellen Infrastrukturquellen einsammeln, kommen bei SOAR noch weitere Faktoren hinzu. So berücksichtigt SOAR beispielsweise externe Informationen wie „Threat Intelligence Feeds" von Sicherheitssoftware-Anbietern oder anderen externen Drittanbietern. Diese Informationen werden benötigt, um ein besseres Gesamtbild

Fazit

Die Cyber-Attacken nehmen jedes Jahr zu, wie die BSI-Studien entsprechend darlegen. Dabei gehen die Angreifer immer raffinierter vor und verlassen sich zunehmend auf digitale Hilfsmittel. Dementsprechend sind Social-Engineering- und Phishing-Angriffe weniger geworden, da hier der Angreifer manuell agieren muss. Das Einschleusen von Schadsoftware über das Internet per E-Mail oder Web-Browser ist hingegen stark ansteigend. Die Opfer sind zudem keine bekannten Unternehmen oder Konzerne mehr, sondern betreffen auch kleinere Unternehmen und Kommunen. Daher muss sich bei der Denkweise von Kommunen und Unternehmen etwas grundlegend ändern: nicht die Verfügbarkeit oder die Effizienz von internen Prozessen sollten allein der Maßstab sein, sondern die IT-Sicherheit immer mitbetrachtet werden. Sie darf nicht mehr nur als Kostenfaktor und Prozess-Hindernis betrachtet, sondern sollte als integraler Bestandteil einer Absicherungsstrategie begriffen werden. Schließlich baut man ja auch kein Firmengebäude ohne Türschlösser und Alarmanlagen, wenn Unternehmenseigentum geschützt werden soll. UTM-Firewall-Systeme sind dabei für den Schutz nicht mehr ausreichend, sondern müssen durch die hier beschriebenen Sicherheitssysteme ergänzt werden. Welche Lösungen hierbei sinnvoll sind, muss individuell geklärt werden, da die vorhandenen Sicherheitssysteme mit den neuen Lösungen zusammenarbeiten sollten. Grundsätzlich lässt sich aber festhalten, dass ein NAC-System als digitale Schutz- und Schließvariante eine sinnvolle Ergänzung darstellt. Darauf aufbauend sollten Lösungen angestrebt werden, die eine intelligente Anomalie-Erkennung besitzen und möglichst nur wirklich relevante Vorfälle melden. Erst dadurch kann ein wirksamer APT-Schutz aufgebaut werden. Ob man nach einer kritischen Anomalie-Erkennung automatisiert das System reagieren oder lieber einen IT-Administrator entscheiden lässt, hängt wiederum von der Firmenphilosophie ab.

***Prof. Dr.-Ing. Kai-Oliver Detken** ist seit dem Jahr 2001 Geschäftsführer der DECOIT® GmbH (www.decoit.de) und Honorarprofessor im Fachbereich Informatik an der Hochschule Bremen. Seine Arbeits- und Forschungsgebiete umfassen Rechnernetze, Internet-Technologien, Voice over IP (VoIP) und IT-Sicherheit. Sein aktuelles „Handbuch Datensicherheit" erschien im Dezember 2020 im KSV.*

Buch-Tipp

Prof. Dr.-Ing. Kai-Oliver Detken,
Prof. Dr.-Ing. Evren Eren
Handbuch Datensicherheit

KSV, 2020
Softcover, 410 Seiten
Euro 69,00
ISBN 9783829314923

Literaturhinweise
[1]: BSI: Die Lage der IT-Sicherheit in Deutschland 2020. Jahresbericht des Bundesamts für Sicherheit in der Informationstechnik (BSI), September 2020, Bonn 2020

[2]: A. Dreißigacker, B. von Skarczinski, G. R. Wollinger: Forschungsbericht Nr. 152: Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019, DruckTeam Druckgesellschaft mbH, Hannover 2020

[3]: K.-O. Detken, C. Kleiner, M. Rohde, M. Steiner: IT-Sicherheitsanalyse durch NAC-Systeme mit SIEM-Funktionalität. D.A.CH Security 2017: Bestandsaufnahme, Konzepte, Anwendungen und Perspektiven, ISBN 978-3-00-057290-6, Hrsg. Peter Schartner und Andrea Baumann, syssec-Verlag, München 2017

[4]: K.-O. Detken, E. Eren: Handbuch Datensicherheit: Datensicherheit in Kommunikation und Information – Handlungsempfehlungen für Kommunen. Handbuch, kartoniert, 410 Seiten, ISBN 978-3-8293-1492-3, Praxis der Kommunalverwaltung, Kommunal- und Schul-Verlag GmbH & Co. KG, Wiesbaden 2020