Gefährdung und Absicherung von IT-Infrastrukturen:

Schutz und Anomalie-Erkennung durch ScanBox

Der Stand der IT-Sicherheitstechnik in Behörden und Unternehmen erstreckt sich heute von Firewalls über Proxys bis hin zu Antiviren-Systemen. Dabei steht meistens die Verfügbarkeit der Betriebsprozesse im Vordergrund und nicht die Analyse der IT-Sicherheit. Neuere Lösungen, wie Network Access Control (NAC), Intrusion Detection System (IDS) oder Security Information and Event Management (SIEM), sucht man daher oftmals noch vergeblich. Dabei hat der Bundesrat im Mai 2021 die Umsetzung des IT-Sicherheitsgesetzes 2.0 gebilligt, welches nicht mehr nur KRITIS-Betreiber in die Pflicht nimmt ihre Sicherheitsmaßnahmen zu verstärken. Daher müssen sich Behörden und Unternehmen zunehmend mit ihrer internen Sicherheit beschäftigen und diese auch überprüfen lassen. Hier setzt das Monitoring- und Security-Analysetool ScanBox an.

Von Prof. Dr. Kai-Oliver Detken, DECOIT GmbH

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 2021 konnte dabei eine Fortsetzung des Trends beobachtet werden, dass Angreifer Schadprogramme für cyberkriminelle Massenangriffe auf Privatpersonen, Unternehmen und Behörden nutzen. Dabei vergrößerte sich die Angriffsfläche durch die verstärkte Nutzung von Remote-Zugängen, Privatgeräten und Videokonferenzsystemen durch die COVID-19-Pandemie erheblich.

ScanBox-Appliance

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 die Nutzung von Hyperlinks auf einen Computer. 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. Dadurch können Daten verschlüsselt und der Zugang zu Systemen eingeschränkt werden, um anschließend ein Lösegeld zu erpressen. Grundsätzlich muss zusätzlich laut BSI in so einem Fall davon ausgegangen werden, dass die Daten dauerhaft kompromittiert bleiben, auch nach einer Lösegeldzahlung. Hinzu kommt ein 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.

Anfang 2021 sorgten zudem vier kritische Sicherheitslücken von Microsoft im MS-Exchange-Server für bundesweites Aufsehen. Diese Lücken wurden für gezielte Angriffe auf die IT-Infrastruktur ausgenutzt und aufgrund der leichten Ausnutzbarkeit mittels Exploit-Kits durch das BSI als extrem kritisch eingestuft. Dies war die zweithöchste der möglichen Krisenstufen! Von den geprüften Systemen erwiesen sich 98 Prozent als verwundbar. Durch das schnelle Handeln der Systembetreiber konnte dieser Anteil innerhalb von zwei Wochen immerhin auf 10 Prozent gedrückt werden. Allerdings war es zu diesem Zeitpunkt bereits für die meisten Institutionen zu spät [1].

© DATAKONTEXT GmbH · 50226 Frechen · <kes> Special KRITIS, Februar 2022

Überwachung der IT-Sicherheit

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 zum Beispiel Unified-Threat-Management-(UTM)-Firewalls oder Antiviren-Systeme, keinen alleinigen Schutz mehr an. Um interne Netz- und Serverzugriffe wirksam schützen zu können, sind daher neue Systeme entwickelt worden, wie IDS-Systeme, die versuchen das interne Netzverhalten zu analysieren, Angriffe durch Muster zu erkennen und gegebenenfalls automatisierte Gegenmaßnahmen einzuleiten. IDS-Systeme sammeln Log- und Netzwerkdaten und bereiten diese Datenflut vornehmlich für IT-Sicherheitsexperten auf, weshalb sie den normalen IT-Administrator oftmals überfordern. Daher konnten sich solche Systeme nicht am Markt durchsetzen.

Die ScanBox (www.scanbox-product.de) der DECOIT GmbH, die auf der leistungsfähigen Appliance des UTM-Herstellers Telco Tech GmbH basiert, setzt auf eine einfachere Handhabung. Die Appliance wird temporär oder permanent an einen Mirror-Port der internen Switches angeschlossen, um aktive oder passive Scans in regelmäßigen Abständen durchzuführen – es ist keine Installation an Client-/Serversystemen erforderlich. Dadurch werden alle IT-Systeme auf Schwachstellen untersucht und diese in Tickets veröffentlicht. Gleichzeitig erfolgt ein Vergleich mit der aktuellen Common-Vulnerabilities-and-Exposures-(CVE)-Datenbank, in der beispielsweise auch der Hersteller Microsoft seine MS-Exchange-Schwachstellen eingestellt hatte. Die Schwachstellen werden von der ScanBox automatisch bewertet (kleines/mittleres/hohes Risiko) und in einem Dashboard übersichtlich dargestellt. Jeder Vorfall (Ticket) wird dabei mit einer leicht verständlichen Handlungsempfehlung versehen, sofern dies möglich ist. Aktive und passive Scans können getrennt voneinander ausgelöst werden, wodurch der Einsatz in IT- und OT-Netzen möglich ist.

Auch bei der ScanBox ist die Datenmenge nicht unerheblich, weshalb nach einem bestimmten Zeitabschnitt (Index-Lifecycle-Management) die interne Festplatte bereinigt wird. Die Daten können dabei auf einem externen Server archiviert oder komplett gelöscht werden. Dabei werden vorhandene Vorfälle (Schwachstellen) im Ticketsystem nicht angetastet. Ausgegeben wird ein monatlicher PDF-Report, der alle Vorfälle auflistet und die Sicherheitsvorfälle dokumentiert. Aktive Scans können zu bestimmten Zeiten durchgeführt werden, um den Betrieb nicht zu stören. Die Anomalie-Erkennung wird regelbasiert vorgenommen, um Abweichungen von der Compliance zu erkennen, da automatisierte KI-Systeme zu viele „False Positives“ erzeugen. Dadurch können auch kleine und mittelständische Unternehmen (KMU) von einem fortschrittlichen SIEM-System profitieren, welches vorher nur Großkunden vorbehalten war.

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 der Angreifer hier manuell agieren muss. Das Einschleusen von Schadsoftware über das Internet per E-Mail oder Webbrowser ist hingegen stark ansteigend. Die Opfer sind zudem nicht nur bekannte Unternehmen oder Konzerne, sondern auch kleinere Unternehmen und Behörden. UTM-Firewall-Systeme sind dabei für den Schutz nicht mehr ausreichend, sondern müssen durch interne Sicherheitssysteme, wie die ScanBox (www.scanbox-product.de) ergänzt werden. Dadurch hätten beispielsweise die CVE-Schwachstellen von Microsoft lange vor der Exchange-Eskalation erkannt werden können. Daher muss sich bei der Sicherheitsdenkweise etwas grundlegend ändern: Nicht die Verfügbarkeit oder die Effizienz von internen Prozessen sollten allein der Maßstab sein, sondern die IT-Sicherheit soll immer mitbetrachtet werden. Sie darf nicht mehr nur als Kostenfaktor und Prozesshindernis betrachtet, sondern sollte als integraler Bestandteil einer Absicherungsstrategie begriffen werden. ■

Prof. Dr.-Ing. Kai-Oliver Detken ist seit dem Jahr 2001 Inhaber und Geschäftsführer der DECOIT GmbH (www.decoit.de) sowie 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-Verlag. Die DECOIT GmbH ist ein IT-Systemintegrator und Softwarehaus, dessen Mission die Bereitstellung, Optimierung, Absicherung und der Support von technischer IT-Infrastruktur sowie die Entwicklung kundenorientierter und innovativer Open-Source-Software-Lösungen ist.

Literatur

[1] BSI, Die Lage der IT-Sicherheit in Deutschland 2021: Jahresbericht des Bundesamts für Sicherheit in der Informationstechnik (BSI), September 2021, Bonn 2021

[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