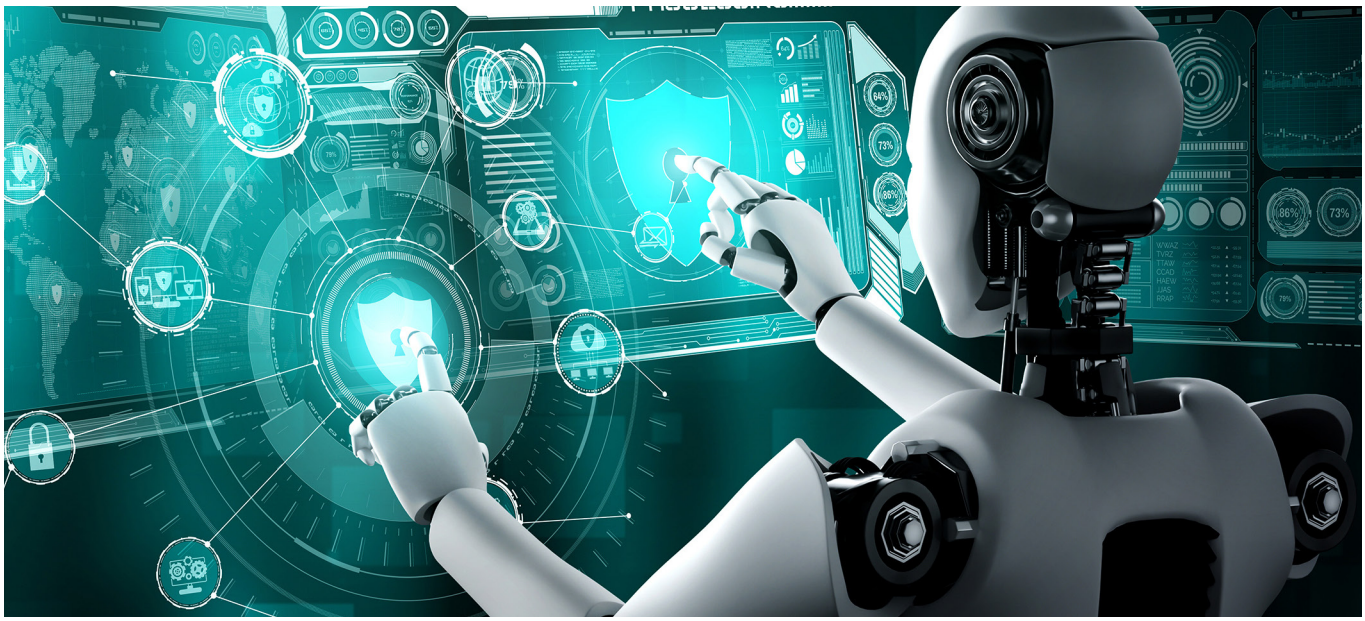
SECURITY INSIDER

Sonderdruck

CASE STUDY ZUR IT-SICHERHEIT

Wie eine KI die KRONEN GmbH vor Cyber-Angriffen bewahrt

Die Einführung der DSGVO 2018 glich einem Paukenschlag. Die KRONEN GmbH sah sich in der Folge mit umfangreichen Anforderungen in Sachen Datenschutz konfrontiert, die mit den vorhandenen Mitteln nicht abzudecken waren. Auf der Suche nach einer Lösung stieß das Unternehmen auf den Systemintegrator Consulting4IT sowie auf dessen Partner, den Software-Hersteller Varonis, der mit seinem Ansatz der Datentransparenz perfekt geeignet war, um die neuen Vorgaben einhalten zu können.



(Bild: Blue Planet Studio - stock.adobe.com)

Während eines ernstzunehmenden Cyberangriffs erwies sich die KI-basierte Software von Varonis bei der Kronen GmbH als Segen.

„Das mit der KI" startete im Hause KRONEN mit den neuen Anforderungen der DSGVO ab 2018. Der Datenschutzbeauftragte Gunter Herbert sah sich mit einer Mammutaufgabe konfrontiert. Denn was sich für Außenstehende einfach und richtig anhört - nämlich personenbezogene Daten zu schützen -, stellte Unternehmen wie die KRONEN GmbH vor eine gewaltige Herausforderung. Herbert war schnell klar: Er musste es schaffen, klare Strukturen in den Daten-Dschungel zu bringen, um den Anforderungen der Nachweispflicht laut DSGVO nachkommen zu können.

In einem Seminar zum Thema Datenschutz wurde ihm die Software von Varonis vorgestellt, die er direkt als brauchbar erachtete. Er ging mit der Idee zu IT-Leiter Frank Wickersheim. Um den Nutzen besser abwägen zu können, lud dieser die Experten des Herstellers zu einer Präsentation ein und schließlich gab auch die Chefetage grünes Licht. „Natürlich war das hinsichtlich der DSGVO ein notwendiger Schritt", meint Wickersheim zur damaligen Entscheidung. „Welche Vorteile uns diese Lösung für die gesamte IT-Security des Unternehmens bringen würde, war für mich damals aber noch nicht klar. Die Lösung schien mir zunächst einmal ein Datenschutz-Tool zu sein, allenfalls eine Art Monitoring-Software. Erst später wurden mir all die Vorteile bewusst, wie beispielsweise die Abwehr von Hacker-Angriffen oder die Transparenz über Datenstrukturen und Berechtigungen."

Laufen lernen mit dem Hightech-Tool

Nach Beauftragung des Systemspezialisten Consulting4IT, einem der wenigen Platinum-Partner von Varonis Deutschland, ging es direkt ans Eingemachte. Der erste Schritt: Die Schaffung einer Grundlage für den korrekten Datenschutz nach DSGVO mittels Aufarbeitung und Auswertung der Daten- und Berechtigungsstrukturen durch die Varonis-Software.

„Wir starteten also mit der Indizierung von Dateien und deckten auf, wo was lag

und wer darauf Zugriff hatte. Dabei kamen zum Teil Dinge ans Licht, bei denen wir ganz schön schlucken mussten“, erinnert sich Wickersheim. Beispielsweise entdeckten sie auf einem Server ein Excel-File mit sämtlichen Kreditkarteninformationen der laufenden Geschäftskreditkarten – theoretisch zugänglich für jeden Mitarbeiter. „Da uns klar war, welches Risiko und welchen Anreiz zum Missbrauch das darstellt, schränkten die Zugriffsrechte ein. Mit diesem Fall und dem Durchspielen diverser Szenarien der Art ‚Was passiert, wenn…‘ haben wir quasi Laufen gelernt. “, erklärt er. „Es machte mich aber bereits zu diesem Zeitpunkt nachdenklich. Denn es wurde offensichtlich, welches Einfallstor wir mit solchen Überberechtigungen auch für externe Angriffe öffneten.“

Umso weiter die Software-Integration fortschritt, desto mehr wurde ihm klar: „Viele Jahre wusste ich auswendig, wo was liegt. Doch mittlerweile haben wir zig Terrabyte an Daten auf unseren Servern liegen und vieles wird über Clouds und Chats verschickt. Da hat kein Mensch mehr den Überblick, auch ich nicht. Erst nach der Implementierung der neuen Software habe ich verstanden, wie wichtig es ist, in Sachen Daten Transparenz zu haben.“

KI trifft Mensch – Von Alerts, Missverständnissen und Verdachtsfällen

Die ersten Monate waren mühsam. „Man musste der KI anfangs bei jedem Datenzugriff sagen: Ja, der darf das und nein, der darf das nicht“, so Wickersheim. Als dann nach etwa sechs Monaten das Gröbste geschafft war, erkannte der IT-Leiter neben der Erfüllung der DSGVO-Anforderungen weitere Vorteile, mit denen er so nicht gerechnet hätte. „Beispielsweise in der Entwicklungsabteilung“, erläutert er. „Hier gibt es einen gemeinsamen Pool an technischen Dateien. Ab und zu kommt es vor, dass an einer Datei etwas verändert wird. In der Regel ist es recht unwahrscheinlich, dass der Server nachts beschließt, aus einem Rohr ein Blech zu machen. Jetzt kann ich lückenlos belegen, was wann von wem geändert wurde. So können Fehlkonfigurationen schnell gefunden und Missverständnisse aus der Welt geräumt werden.“

Noch wichtiger ist für ihn, dass auf diese Weise auch Insiderbedrohungen wirksam der Riegel vorgeschoben wird. Denn sollte doch einmal jemand absichtlich Unterlagen sabotieren oder entwenden wollen, kann dies lückenlos nachvollzogen und aufgeklärt werden. „Es geht hierbei nicht um das Ausspionieren von Mitarbeitern“, betont er. „Der Vorteil ist einfach der, dass man in konkreten Verdachtsfällen direkt feststellen kann, ob hier was dran ist oder eben nicht.“

Feuerprobe bestanden – Geohopping-Angriff entlarvt

Anfang des Jahres 2022 bekam die KI Gelegenheit, sich auch hinsichtlich eines Angriffs von außen aktiv zu bewähren. Wickersheim nickt nachdrücklich, als er sich daran erinnert: „Ein Kollege hat sich morgens am Standort in Kehl eingeloggt. Und 20 Minuten später plötzlich aus Lagos. Solange es noch keine Beam-Technologie gibt, ist das einfach nicht möglich. Die KI hat das sofort erkannt und den Account gesperrt. Der Angreifer kam nicht einmal in die Nähe sensitiver Daten.“

(Bild: KRONEN GmbH)

Frank Wickersheim, IT-Leiter der KRONEN GmbH.

Sofern es bis zu diesem Zeitpunkt noch Vorbehalte gegen die Software gegeben hätte, wären diese damit endgültig zerschlagen worden. Denn ohne das automatische Eingreifen der KI hätte aus diesem Geohopping-Ereignis durchaus ein kritischer Vorfall werden können. Wickersheim ist deshalb heilfroh, dass die Kronen GmbH sich bereits frühzeitig für diese Lösung entschieden und damit ein solides Sicherheitsnetz für ihre IT-Infrastruktur geschaffen hat.

Wie KRONEN sich weiter schützt und strukturiert

Um das Schutzschild weiter zu verstärken, hat Wickersheim weitere Maßnahmen ergriffen. Beispielsweise wird nun bei einer bestimmten, stark gehäuften Anzahl an Datenänderungen in einem definierten Zeitraum der ausführende Account direkt gesperrt. Schließlich liegt bei solchen Aktivitäten der Verdacht nahe, dass Ransomware zugange ist.

Was er mittlerweile ebenfalls sehr zu schätzen weiß: Die Möglichkeit zur Bewertung von Online-Vorgängen. Denn schließlich laufen längst nicht mehr alle Datenströme nur intern. Stattdessen werden diese über Chats und Clouds auch mit externen Personen geteilt. „Davon würde ich ohne unsere Security-Software gar nichts mitbekommen“, gibt Wickersheim zu Bedenken. „Mit ihr erkenne ich, wie die Berechtigungsstrukturen in diesem Umfeld aufgebaut sind und kann mittels definierter Regeln steuernd eingreifen.“

Wickersheim ist nun dabei, die aktive Arbeit mit dem Tool weiter auszubauen. „Anfangs ging es darum, die DSGVO umzusetzen. Dann wollten wir die ‚Kronjuwelen‘ des Unternehmens schützen. Jetzt gehen wir in die Details und stricken das Netz immer dichter.“

Warum es besser ist, klein anzufangen

Auf die Frage, was er heute bei der Implementierung anders machen würde, antwortet er: „Wir haben direkt mit dem großen Datenserver angefangen. Das würde ich so nicht mehr tun, da das Anlernen der KI aufgrund der Datenmenge relativ lange gedauert hat. Stattdessen macht es Sinn, mit einem kleinen Server zu starten. Die KI kann auf diese Weise effektiver lernen und schnellere Fortschritte erzielen.“

Das Thema Akzeptanz bei den Mitarbeitern ist laut Wickersheim auch nicht zu vernachlässigen. Sein Tipp: „Man muss den Leuten die Sinnhaftigkeit der Lösung nahebringen und klarstellen, dass diese das Unternehmen und damit auch seine Mitarbeiter vor kriminellen Cyber-Machenschaften schützt."

Außerdem, so Wickersheim, sollte man bei einem solchen Projekt stets Wert auf einen erfahrenen und spezialisierten Systemintegrator legen. Die Consulting4IT war für ihn, neben dem Support durch den Hersteller selbst, mit ausschlaggebend für den Erfolg des Projekts.

KRONEN und Varonis – Liebe auf den zweiten Blick

Wickersheim resümiert: „Am Anfang habe ich in der KI-Lösung nicht viel mehr als ein Tool für den Datenschutz gesehen. Doch mit der Zeit hat es mich immer wieder aufs Neue positiv überrascht und immer mehr Möglichkeiten offenbart. Jetzt gibt mir das Tool als solider IT-Security-Baustein Sicherheit im Arbeitsalltag. Mit der Software kann ich einen extrem hohen Sicherheitsstandard gewährleisten und dafür sorgen, dass es Personen mit unlauteren Absichten so schwer wie möglich haben – ein entscheidender Vorteil im Kampf gegen Cyber-Kriminelle."

Wie das Projekt von KRONEN zeigt, braucht es manchmal etwas Zeit, bis die Arbeit Früchte trägt. Oder - anders ausgedrückt - ab und zu ist es eben Liebe auf den zweiten Blick, die zu einer erfolgreichen Beziehung führt. Man kann es sehen, wie man will. Die neue KI-Lösung wurde zu einem echten Bollwerk der IT-Verteidigung für die KRONEN GmbH, quasi zum Verteidiger der Krone. Und Wickersheim schließt im Brustton der Überzeugung: „Ich möchte sie nicht mehr missen."

ÜBER DIE KRONEN GMBH

Das 1978 gegründete Unternehmen KRONEN GmbH mit Sitz im süddeutschen Kehl zählt zu einem der führenden Maschinenbauer in der Freshcut-Industrie. Dabei hat sich die Kronen GmbH auf die Entwicklung, Produktion und Lieferung von Einzel- und Sondermaschinen sowie hochtechnisierten Prozessanlagen im Bereich der Salat-, Gemüse- und Obstverarbeitung spezialisiert. Mit Vertretungen in über 80 Ländern weltweit und Lieferungen in mehr als 120 Länder hat sich das Unternehmen in der Lebensmittelbranche einen Namen gemacht und erreichte 2021 trotz pandemiebedingt angespannter Marktlage einen Rekordumsatz von 18,5 Millionen Euro.

(Bild: KRONEN GmbH)

Hauptstandort der KRONEN GmbH in Kehl-Goldscheuer am Rhein.

KRONEN® DIE KRONE FÜR FRISCHE

CONSULTING4IT

VARONIS Platinum Partner

15.02.2023 | Autorin: Linda Schmittner

Consulting4IT GmbH - Telefon: +49 (0) 7243 2058 500 - E-Mail: info@consulting4it.de