Sicherheit und KI

„Man muss sich überlegen, was schützenswert ist“

LHIND-Sicherheitsexperte Christian Garske über die aktuellen Gefahren für Unternehmen und wie Kriminelle von KI profitieren.

→ INTERVIEW: KONSTANTIN PFLIEGL

ZUR PERSON

Christian Garske ist Business Manager Security & Privacy Consulting beim IT-Dienstleister Lufthansa Industry Solutions (LHIND). Der Diplom-Wirtschaftsinformatiker begann dort 2008 als IT-Berater im Technologiecenter in Oldenburg. 2010 wechselte er in die Business-Units Industry & Automotive und Technology Consulting nach Norderstedt und spezialisierte sich dort auf die Themen Sicherheitsberatung und Sicherheitslösungen.

Auch im Jahr 2022 bleibt IT-Sicherheit für Unternehmen eines der wichtigsten Themen. Laut Studien des Digitalverbands Bitkom haben Cyberangriffe bei 86 Prozent der Unternehmen in Deutschland zuletzt einen Schaden verursacht – die Wucht, mit der insbesondere Ransomware-Angriffe die Wirtschaft erschütterten, sei besorgniserregend und treffe Betriebe aller Branchen und Größen, resümiert der Verband. Die Schäden durch Erpressung, verbunden mit dem Ausfall von Systemen oder der Störung von Betriebsabläufen, seien seit 2019 um rund 360 Prozent gestiegen.

Darauf müssen Unternehmen reagieren. Doch wie sehen die konkreten Gefahren aus und wie rüsten sich die Firmen vor Angriffen? com! professional spricht darüber mit Christian Garske, Business Manager für den Bereich Security Consulting beim IT-Dienstleister Lufthansa Industry Solutions (LHIND).

> „Die Dinge, die den Geschäftszweck befördern, müssen dicht sein.“

com! professional: Herr Garske, wenn man sich die aktuellen Zahlen des Bitkom anschaut, dann stellt sich die Frage, ob Unternehmen die IT-Security überhaupt noch so kontrollieren können, dass sie ohne Schäden davonkommen.

Christian Garske: Ohne Schäden – nein. Kann man aber etwas tun, um die Schäden so gering wie möglich zu halten? Definitiv. Die wichtigste Frage ist: Was tut denn wirklich weh? Und genau da muss man ansetzen. Wenn man mit der Annahme loslaufen würde, ich schaffe 100 Prozent Sicherheit, dann wird das sehr schnell unwirtschaftlich. Als Unternehmen muss ich daher überlegen, was wirklich schützenswert ist und welche Folgen eine Störung hätte.

com! professional: Zum Beispiel die Produktion …

Garske: Die Dinge, die im Endeffekt den Geschäftszweck befördern, müssen dicht sein, und an dieser Stelle muss der höchste Schutz gewährleistet sein.

Das kann man sich vorstellen wie bei einer Zwiebel: Wenn die äußere Schale mal eine Schramme abbekommt, dann ist das nicht so schlimm. Wenn allerdings der Zwiebelkern durchstoßen wird, dann ist das nicht mehr so gut. Und ähnlich sieht es bei einem Unternehmen aus. Man muss sich überlegen, welche Dinge definitiv nicht umfallen dürfen, weil es ansonsten sehr wehtut.

Das Problem beginnt dann, wenn ein Angreifer zuschlägt und er irgendeine Lücke findet. Ihm reicht eine einzige – und in jedem Unternehmen gibt es unzählige potenzielle Lücken. Aber wenn ich wie bei der Zwiebel mehrere Schutzzonen baue, bekomme ich es mit, wenn jemand angreift. Was dabei entscheidend ist: Ich muss es sehr früh sehen, denn dann kann ich direkt etwas dagegen tun. Wenn ich weiß, dass der Angreifer irgendwo eine Hürde genommen hat, habe ich im Zweifelsfall nur einen Mini-Schaden oder vielleicht ist auch noch gar →

Bild: Lufthansa Industry Solutions


„Unternehmen sind wie eine Zwiebel: Wenn die äußere Schale mal eine Schramme abbekommt, dann ist das nicht so schlimm. Wenn allerdings der Zwiebelkern durchstoßen wird, dann ist das nicht mehr so gut."

nichts passiert. Und ich kann den Angreifer überwachen. Entweder lasse ich ihn im Kreis laufen oder ich schmeiße ihn gleich raus. Dass Unternehmen gar nicht angegriffen werden oder jeden Angriff hundertprozentig abgewehrt bekommen, das wird es nicht geben. Wenn ich es aber schaffe, engmaschige Fangnetze zu bauen, und entsprechend reagiere, dann werde ich die Angreifer los, bevor sie ernsthaften Schaden anrichten können.

„Dass Unternehmen gar nicht angegriffen werden oder jeden Angriff hundertprozentig abgewehrt bekommen, das wird es nicht geben."

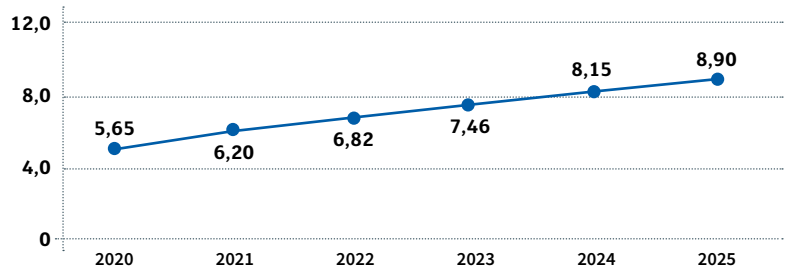
com! professional: Um bei Ihrem Bild zu bleiben: Den Zwiebelkern muss ich sichern – und nach außen hin muss ich mit ein paar Kollateralschäden leben. Diese lassen sich aber nicht ohne immensen finanziellen Aufwand abwehren, oder?

Garske: Als Erstes muss ich mir als Unternehmen überlegen, wie digital ich eigentlich bin. IT-Risiken sind eine Klasse von Risiken, die ein Unternehmen nun mal hat. Und wenn ich ein besonders digitales Unternehmen bin, ist diese Risikoklasse besonders gewichtig. Wenn mein Unternehmen weniger digital ist, dann ist das eine eher unwichtige Kategorie.

Als extremes Beispiel kann man eine Currywurst-Bude nehmen: Was gibt es da an IT? Vielleicht eine Excel-Abrechnung für die Tageseinnahmen, das war's. Häufig wird dafür auch noch ein Privatrechner verwendet und kein Firmengerät. Das entscheidende Problem bei der Bude ist, dass ausreichend Currywürste auf dem Grill liegen.

Markt für IT-Sicherheit in Deutschland

Ausgaben für Software, Hardware und Dienste im Bereich IT-Sicherheit: Sie stiegen 2021 im Vergleich zum Vorjahr um 9 Prozent – Tendenz steigend.



com! professional 2/2022 Angaben in Milliarden Euro; Quelle: Bitkom/IDC

com! professional: Auf der anderen Seite gibt es Unternehmen, die von digitalen Dienstleistungen leben …

Garske: Dann wäre es fatal, wenn man hier nicht in die Absicherung der digitalen Mittel investieren würde. Denn wenn die umfallen, dann habe ich kein Geschäft mehr. Man muss genau austarieren, wo man als Unternehmen steht. Das ist auch das, was ich die CEOs der Unternehmen oft frage: Seid ihr in den letzten fünf oder zehn Jahren digitaler geworden? Und im Regelfall antworten sie mit Ja. Wenn ich als Unternehmen merke, dass ich digitaler werde, dann muss ich mir die Frage stellen: Was habe ich denn parallel auch im Bereich der IT-Security gemacht?

com! professional: Was sind denn aktuell überhaupt die größten Risiken für Unternehmen? Man hört meist von Ransomware. Welche weiteren Gefahren gibt es? Sind Ransomware-Angriffe momentan tatsächlich die gefährlichsten Szenarien – oder gelangen andere Angriffe schlicht nicht so oft an die Öffentlichkeit?

Garske: Ransomware ist das Offensichtlichste. Das ist in den letzten Jahren, vor allem vom Monetarisierungseffekt her, für die Angreifer am lohnendsten gewesen. Was es daneben noch häufig gibt, ist das sogenannte Krypto-Mining. Das heißt, man klaut einfach Rechenkapazität von seinem Opfer und lässt sich damit Bitcoins oder eine andere Kryptowährung errechnen. Wenn man den Strom nicht selber bezahlen muss, sondern das Opfer dies tut, dann ist das für den Angreifer lohnend. Er streicht nur den Gewinn ein. Die dritte große Kategorie ist aus meiner Sicht ein eher klassisches, aber nach wie vor aktuelles Thema – Industriespionage.

com! professional: Und wie können sich Unternehmen nun für diese Ernstfälle vorbereiten? Man hat den Eindruck, dass es bei den Unternehmen da draußen hauptsächlich darum geht, Schaden zu minimieren, wenn schon etwas passiert ist … Sind also Unternehmen mangels Vorbereitung in gewisser Weise auch selbst schuld, wenn ein Angreifer sie erfolgreich attackiert?

Garske: Schlechte Vorbereitung erhöht definitiv die Wahrscheinlichkeit, dass mal jemand eindringt. Doch was muss ein Unternehmen tun? Zumindest braucht es saubere Backups – nicht als Online-, sondern als Offline-Backups. Denn wenn ich keine Offline-Backups habe, dann bin ich spätestens bei einem Ransomware-Befall schnell in einer schwierigen Situation. Wenn auch die Backups mitverschlüsselt werden – was will ich dann wiederherstellen? Dann kann ich entweder wieder von vorne anfangen oder ich muss bezahlen. Und jedes Mal, wenn die Angreifer tatsächlich bezahlt werden, befördert dies das Geschäftsmodell.

com! professional: Wie sehen denn da Ihre Erfahrungen aus? Zahlen viele Unternehmen in der stillen Hoffnung, damit schnell wieder aus dem Schlamassel herauszukommen? ➔

OFFICE IST.
WO EIN EIZO IST.

Gebaut für jedes Office – egal, ob zu Hause oder in der Firma: FlexScan-Monitore von EIZO.
Mit größter Anschlussvielfalt, bester Bildqualität und vielen praktischen Ergonomie-Features.
Mehr auf eizo.de/home-office.

Working with the Best

EIZO®

Garske: Öffentliche Statistiken dazu gibt es meines Wissens nicht. Was ich aber so aus dem Markt mitbekomme, ist, dass einige zahlen – immer dann, wenn es nicht anders geht. Wenn jedoch entsprechende Wiederherstellungsmöglichkeiten vorhanden sind, dann kommt man ums Zahlen herum. Stellenweise gelingt die Entschlüsselung auch mal, das ist allerdings ziemlich schwierig.

com! professional: Sie haben die Backups angesprochen. Es gibt also durchaus Möglichkeiten zur Vorsorge. Wie kommt es dann, dass Unternehmen das Thema Sicherheit zwar in der Regel auf dem Radar haben, die Zahl der Angriffe und Schäden aber trotzdem steigt? Wo hakt es? Sind es schlicht die falschen Sicherheitsstrategien?
Garske: Das hat mehrere Gründe: Zum einen spielt sicher die technologische Komplexität eine Rolle, daneben entwickeln sich die Skills und Werkzeuge der Angreifer weiter, aber oft ist es auch fehlende Awareness. Auf der anderen Seite sind es vermehrt die kleineren Mittelständler, die bei den Angreifern im Fokus stehen, weil sie nicht die großen IT-Abteilungen haben.

„Was ich so aus dem Markt mitbekomme, ist, dass einige zahlen – immer dann, wenn es nicht anders geht."

com! professional: Und was ist mit dem Faktor Mensch?
Garske: Er ist ein ganz entscheidender Baustein in dem Spiel. IT-Sicherheit ist ja kein rein technisches Problem. Es gehören auch Menschen und Prozesse dazu. Wenn meine Prozesse nicht funktionieren, dann kriege ich das Unternehmen nicht gesteuert. Wenn meine Menschen, die an den Prozessen beteiligt sind, nicht funktionieren, dann hilft mir auch das ausgeklügeltste Sicherheitskonzept nicht. Die einfachste Tür in ein Unternehmen ist noch immer der Mitarbeiter. Wenn ich zum Beispiel einen Mitarbeiter anrufe, dann bin ich schon mal hinter der Firewall.

com! professional: Was hilft hier? Zero Trust, also grundsätzlich erst einmal niemandem zu trauen?
Garske: Zero Trust ist ein wichtiges Prinzip zur Verbesserung der IT-Sicherheit. Die klassische Burgwallmentalität – hinter der Firewall passiert uns nichts – ist überholt. Das Thema Zero Trust ist in deutschen Unternehmen aber noch nicht in der Fläche da. Zero Trust wird uns mittel- und langfristig helfen.

com! professional: Sollte man es dann mit Künstlicher Intelligenz versuchen? Kann sie dabei helfen, Sicherheitsrisiken zu minimieren beziehungsweise Angriffe rechtzeitig zu erkennen – oder wird KI in der Security zu sehr gehypt?
Garske: Beides. Eine gut eingestellte KI kann sicherlich ganz viele Indizien liefern, an welchen Stellen gerade etwas schiefläuft. Besonders das Alarm-Pushing kann mit einer Künstlichen Intelligenz ganz gut funktionieren. Die Frage ist halt immer, ob es ein echter Alarm ist oder ein False Positive. Eine schlecht trainierte KI sorgt dafür, dass gerade für die nachgelagerten Einheiten, die ohnehin schon sehr viel zu tun haben, noch mehr Arbeit anfällt. Spätestens dann, wenn die Analysten den ganzen Tag damit beschäftigt sind, False Positives wegzuklicken, entstehen Frustrationen. Eine gut trainierte KI, die auch wirklich diesen Entlastungseffekt bringt, hilft natürlich. Aber man muss immer schauen: Für welchen Zweck brauche ich was? Und ich muss das dann auch ausprobieren. Einfach blind etwas von der Stange zu kaufen, weil KI draufsteht, das ergibt keinen Sinn.

com! professional: Das Problem ist, dass auch Cyberkriminelle KI schon lange für sich entdeckt haben …
Garske: Alles, was in der Defensive passiert, passiert auch in der Offensive.

com! professional: Wie nutzt Künstliche Intelligenz den Angreifern? Und für was setzen sie KI ein?
Garske: Auch Kriminelle müssen sich überlegen: Welches Ziel möchte ich eigentlich angreifen? Wenn sie eine KI zum Beispiel für eine Art Vorselektion einsetzen können, wo sich ein Eindringen lohnen könnte, dann ist das schon mal eine ganz spannende Geschichte. Wenn sie wissen, wo sich ein Angriff lohnt, dann ist der nächste Schritt, sich das Waffenarsenal zu überlegen. Je genauer das Feintunen klappt, desto besser natürlich und desto geringer das Risiko erwischt zu werden. Wenn der Angriff läuft, dann hilft alles, was dabei unterstützt, ein Verständnis dafür zu entwickeln, wie das Opfer eigentlich aussieht und welche Verteidigung umgangen werden muss. Am Anfang sieht man ja nur die Haustür. Aber als Angreifer will man ja verstehen, wie die dahintergelagerten Strukturen aussehen und wie man diese schädigen kann.

com! professional: Wenn Unternehmen KI einsetzen, dann kommen zum Beispiel große Security-Anbieter mit entsprechender Infrastruktur zum Einsatz. Aber wie hat man sich das bei Cyberkriminellen vorzustellen? Setzen die ihre eigenen Cloud-Server mit selbst programmierten KI-Diensten auf? Oder buchen sie sich anonym Hyperscaler-Dienste und missbrauchen diese?
Garske: Beides. Eine KI ist erst mal nur ein Baustein, der zum Guten wie zum Schlechten genutzt werden kann. Das Schwierige an einer Künstlichen Intelligenz ist meist nicht die KI selbst, sondern das Trainieren des Modells. Das ist das, was die meisten Leute in meinen Augen völlig unter-

schätzen. Wenn die KI erst einmal läuft, dann nimmt sie einem Arbeit ab. Wenn ich hingegen eine neue KI aufsetze, dann ist das ganz viel manuelle Arbeit. Ich muss zunächst meine Daten bereinigen. Wenn ich dieses sogenannte Clearing einmal abgeschlossen habe, dann kann ich mir überlegen, mit welchen Hypothesen ich meine KI füttere. Und wie bekomme ich die Daten überhaupt dort hinein? Sind das strukturierte oder unstrukturierte Informationen, oder in welcher Taktung kommen sie?

All das hat Einfluss darauf, welche Art von KI ich überhaupt einsetzen kann. Wenn die Art von KI feststeht, dann fange ich mit dem Modelltraining an. Und je besser das Modell ist, desto besser ist der Output der KI.

com! professional: Klingt nach einem hohen Aufwand …
Garske: Wenn ich als Angreifer einen sogenannten One-Shot-Angriff fahre, dann brauche ich keine KI dafür. Wenn ich aber bestimmte Angriffe öfters machen will und dafür nur die Input-Daten variieren muss, ansonsten aber immer ein ähnlicher Angriff abläuft, dann lohnt sich das – zum Beispiel bei Spammern, die ihre E-Mails an den Filtern vorbeibekommen wollen.

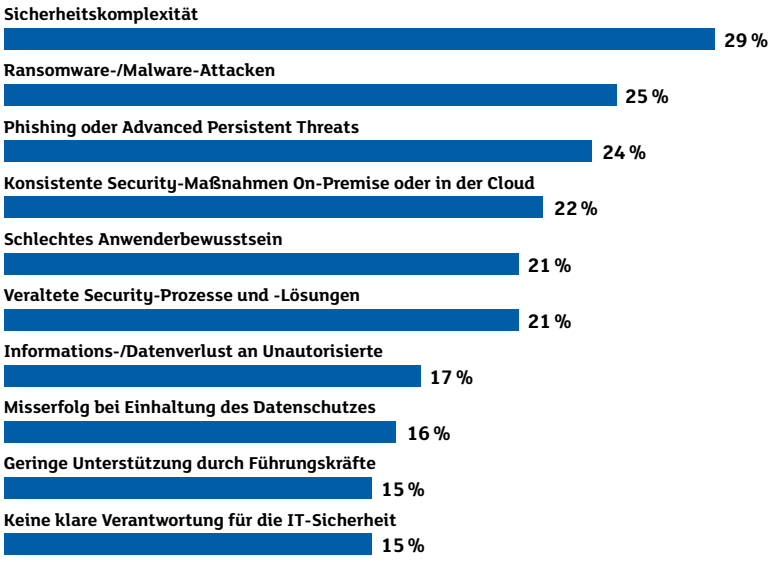
com! professional: Mittelfristig kommen Unternehmen also um eine KI für die IT-Sicherheit nicht herum – allein schon, um gegenüber den Kriminellen quasi eine Patt-Situation herzustellen?
Garske: Das kann man so sagen. Das Datenvolumen, das Unternehmen mittlerweile handeln müssen, ist wahnsinnig groß. Das bedeutet, alles was ich vorweg selektieren kann, was ich vorher quasi in die richtige Schublade packe, das hilft mir.

com! professional: Kommen wir zum Schluss noch kurz auf die kritischen Infrastrukturen zu sprechen. Sie sind im Hinblick auf Angriffe besonders gefährdet und ein Ausfall hat weitreichende Folgen. Das Bundesamt für Sicherheit in der Informationstechnik hat das IT-Sicherheitsgesetz 2.0 auf den Weg gebracht. Es legt nicht nur strengere Vorgaben für Betreiber kritischer Infrastrukturen fest, sondern enthält erstmals auch Vorschriften für Unternehmen von besonderem öffentlichen Interesse. Das klingt doch erst einmal gut, oder?
Garske: Klingt gut, ist aber mal wieder eine juristische Kopfgeburt.

com! professional: Woran mangelt es Ihrer Ansicht nach beim IT-Sicherheitsgesetz 2.0 konkret?

Die größten IT-Sicherheitsherausforderungen in Unternehmen

IT-Sicherheit ist komplex: Für knapp ein Drittel der Unternehmen in Deutschland ist das ein Problem. Zweithäufigste Sorge: Attacken durch Schad-Software.



com! professional 2/2022 Quelle: IDC-Studie „Cybersecurity in Deutschland 2021"

Garske: Ein neuer Aspekt in der Novelle des Sicherheitsgesetzes ist zum Beispiel das Thema Supply-Chain. Man sieht Unternehmen jetzt nicht mehr als frei schwebendes Stückchen Organisation im luftleeren Raum, sondern wir haben eine immer stärkere Vernetzung von Lieferketten. Wenn ein Zulieferer nicht funktioniert, dann kann zum Beispiel Volkswagen keine Autos bauen, weil etwa Chips fehlen.

Ähnlich sieht es in der IT-Sicherheit aus: Wenn mein Provider einen Fehler macht, ich aber seinen Daten vertraue und mich auf ihn verlasse, dann kann aufgrund dieser Vertrauensbeziehung ein Schaden entstehen.

Und genau das will die Novelle des Sicherheitsgesetzes regeln – dass wir in den Provider- und Zulieferbereich stärker hineinschauen können. Aber: Die Regelungen sagen mir natürlich nur, dass ein Unternehmen auf dem Papier ordnungsgemäß arbeitet – nicht aber, dass es das in der Praxis auch tatsächlich tut. Ob ein Zulieferbetrieb wirklich zuverlässig und ordnungsgemäß arbeitet, stelle ich nur durch ein regelmäßiges Monitoring fest. •

„Das Schwierige an einer Künstlichen Intelligenz ist meist nicht die KI selbst, sondern das Trainieren des Modells. Das ist das, was die meisten Leute in meinen Augen völlig unterschätzen."