»Es gibt nur eine echte Sicherheitslösung gegen Cyberangriffe: die kontinuierliche Analyse aller IT-Systeme«

Matthias Nehls
Vorstand der DGC AG

Hackerangriffe nehmen drastisch zu, gleichzeitig unterhalten Unternehmen immer komplexere IT- und Softwarestrukturen. Matthias Nehls, Vorstand der DGC AG, erläutert, warum eine kontinuierliche Überwachung aller Systeme und Schwachstellen immer wichtiger wird, um Erpressungen und Reputationsschäden vorzubeugen.

Herr Nehls, wie ist die gegenwärtige Cyberbedrohungslage in Deutschland?
Unternehmen werden verstärkt angegriffen. Gleichzeitig stellen wir fest, dass viele betroffene Kunden nicht auf die Behörden zugehen. Sie fürchten die riesigen Reputationsschäden, wenn sie angegriffen wurden. Wir dagegen arbeiten aktiv und sehr vertraulich mit den Ermittlungsbehörden zusammen. Dass die Cyberattacken zunehmen, hat mit der komplexen Gemengelage zu tun. Es gibt immer mehr Hackergruppen, die geopolitische Lage ist schwierig – und natürlich ist die Erpressung von Unternehmen ein superlukratives Geschäft, um an Geld zu kommen. Laut dem aktuellen Hiscox Cyber Readiness Report ist die Zahl der angegriffenen Unternehmen in Deutschland von 46 Prozent im Jahr 2022 auf 58 Prozent im Jahr 2023 gestiegen. Diese Angriffe lassen sich also nicht mehr unter den Teppich kehren.

Wieso nehmen Cyberangriffe zu?
Unternehmen, die erpresst werden, bezahlen durchschnittlich eine Million Dollar Lösegeld. Und jedes siebte Unternehmen zahlt. Das Ganze ist also ein lukratives Geschäft. Auf der anderen Seite werden die IT-Systeme immer komplexer. Immer mehr Daten liegen auf Servern von Dienstleistern. Wenn Unternehmen über unser Security-Portal cyberscan.io den Sicherheitscheck machen und dann etliche zum Teil schwerwiegende Schwachstellen angezeigt bekommen, sagen sie immer: Aber das sind ja gar nicht unsere Daten. Die werden doch von einem Partner verwaltet. Man muss jedoch klipp und klar sagen: Daten lassen sich nicht delegieren. Unternehmen müssen dafür Sorge tragen, dass ihre Systeme und die Systeme ihrer Partnerunternehmen tagtäglich sicher sind.

Wie kann man sich gegen Angriffe wappnen?
Wir müssen wieder eine bessere Übersicht über alle IT-Systeme erlangen. Ich vergleiche das gerne mit einem Heißluftballon, der von oben sieht, was unten eigentlich los ist. Mit der zunehmenden Schatten-IT, mit nicht richtig gewarteten Websites und Systemen haben viele Unternehmen aber längst die Übersicht über ihre eigene IT verloren. Unternehmen wissen nicht, welche Systeme überhaupt bei ihnen laufen, welche Versionen installiert sind oder wann Back-ups erfolgen. Dazu kommt, dass Software nur unzureichend aktualisiert wird. Viele Unternehmen bekommen ihre Websites von Agenturen gebastelt, die dann aber nicht mehr die Sicherheit kontrollieren. Und seit dem KI-Hype glauben viele, die perfekte Lösung gefunden zu haben. Das ist ein Trugschluss, der sehr teuer werden kann. Denn: KI allein kann keine Sicherheit garantieren. Menschen sehen noch immer mehr. Deswegen setzen wir auch auf Spezialisten, die Schwachstellen noch besser finden und schneller schließen können.

Und wer sollte sich vor allem wappnen?
Eigentlich sollte natürlich jeder besser und umfassender seine Systeme warten und entsprechend vorsichtig mit Daten umgehen. Was in vielen Unternehmen erstaunlich ist, ist der lasche Umgang mit der Zwei-Faktor-Authentifizierung. Während Enduser die praktisch überall benutzen, wird sie von vielen Administratoren überhaupt nicht genutzt. Gerade Admins müssten viel öfter ihre Zugangsdaten ändern. Das tun sie aber nicht. Ein weiterer wichtiger Punkt sind die Homeoffice-Zugänge. Nach der Corona-Pandemie lässt sich das Rad nicht zurückdrehen. Unternehmen sollten trotzdem sicherstellen, dass ihre Mitarbeitenden zu Hause beispielsweise ihre Fritz-Box auf dem neuesten Stand haben. Auch via Chats und sozialer Medien kommt es immer öfter zu Betrugsfällen, Datenklau und Erpressungsversuchen dank der persönlichen Transparenz, die Mitarbeitende freiwillig in den sozialen Medien schaffen. Das ist eine hervorragende Quelle für Social Engineering.

Unternehmen müssen also bei der Abwehr von Cyberattacken alle Strukturen, auch von externen Dienstleistern, unter einen Hut bekommen und analysieren?
Richtig. Das ist eine komplexe Aufgabe, der wir uns stellen. Wir versuchen, Klarheit in diese komplexen Strukturen zu bekommen. Das Hauptproblem ist ja, dass die Cybersicherheit nicht greifbar ist. Man redet darüber, aber wie und wo diese Sicherheit hergestellt wird oder eben verwundbar ist, lässt sich für viele nicht greifen.

Sie haben mit cyberscan.io ein eigenes Tool entwickelt. Wie funktioniert es?
Wir scannen mit diesem Tool schnell jede eingegebene Infrastruktur. Und Sie sehen dann sofort, wo es leichte, mittlere oder erhebliche Sicherheitslücken gibt. Kundinnen und Kunden wundern sich oft, was wir alles lokalisieren und anzeigen können. Besonders Legacy-Systeme und deren Hardware haben ein extrem hohes Gefahrenpotenzial. Aber das ist typisch für Deutschland. Während junge Unternehmen natürlich nur die neuesten Systeme haben, gibt es beispielsweise in Stahlbauunternehmen über Jahrzehnte gewachsene Altsysteme, auf denen unglaublich alte Software läuft. Teilweise müssen da Mitarbeiter aus der Rente geholt werden, weil keiner weiß, wie die bedient werden.

> **„Nur eine kontinuierliche und ganzheitliche Überwachung aller Systeme garantiert Sicherheit.**

Was ist die Besonderheit bei cyberscan.io?
Sie erkennen als Unternehmen plötzlich, wie Infrastrukturen angegriffen werden können. Mitunter sehen Sie, wie leicht E-Mails und Passwörter zu entschlüsseln sind. Teilweise laufen auch Systeme, die schon 2002 installiert wurden und seitdem im Grunde nicht überprüft oder angepasst wurden. Selbst bei so prominenten Adressen wie bund.de haben wir rund 360 Schwachstellen identifiziert. Unser Tool macht auch klar, wie leicht ein Reputationsschaden entstehen kann. Denken Sie nur an die Datenlecks beim DFB oder bei Motel One. Es gibt Unternehmen, die einen solchen Gau mit der Veröffentlichung sämtlicher Zugangs- oder Kundendaten nicht verkraften. Man muss es deutlich sagen: Cybersecurity ist auch aktiver Markenschutz

Ihr Tool hilft auch, Gefahren zu visualisieren. Das heißt, es trägt auch zum Verständnis von Cyberattacken bei?
So ist es. Wir zeigen live und in Farbe, wo der Datenschutz nicht funktioniert oder die IT-Security schlecht gegen Angriffe gerüstet ist. Wir bilden dabei bei internationalen Unternehmen auch die weltweite IT- Struktur ab. Unser Check zeigt häufig, dass Geld und neue Tools gebraucht werden, um die Sicherheit zu verbessern.

Was empfehlen Sie Unternehmen hinsichtlich einer optimalen Absicherung?
Nur eine kontinuierliche und ganzheitliche Überwachung aller Systeme garantiert Sicherheit. Wir wollen deshalb auch ein Bewusstsein für die Wichtigkeit der Security-Verantwortlichen schaffen. Das sind eben nicht irgendwelche Nerds oder merkwürdigen Typen. Sie sind es, die für die zwingend notwendige Cybersicherheit in den Unternehmen sorgen. Im Grunde sind das die wahren Helden im Unternehmen. Und wir unterstützen sie mit unserer langjährigen Expertise geräuschlos im Hintergrund.

Inwieweit spielen alle Mitarbeitenden eine Rolle, wenn es um die kontinuierliche Analyse und Abwehr von Cyberattacken geht?
Natürlich müssen Mitarbeitende für die Gefahren von Cyberangriffen sensibilisiert werden, das ist gar keine Frage. Aber man muss auch sagen, dass Unternehmen ihre Sicherheitsprobleme nicht komplett auf die Mitarbeitenden abwälzen können. Die Mitarbeitenden sind sicher das schwächste Glied in der Abwehrkette, wenn es etwa um Social Engineering geht, um Daten, die mit anderen Leuten leichtfertig geteilt werden. Hier sind intensive Schulungen erforderlich. Aber der Überbau muss stimmen, er muss stark sein. Die einzig echte Sicherheitslösung ist die kontinuierliche Analyse und das entsprechende Updaten aller Systeme.

Interview **Rüdiger Schmidt-Sodingen**

DGC AG