

INHALTSVERZEICHNIS

OHNE RUBRIKEN

Vernetzung ist Einfallstor für Hacker

3

Allgemeine Zeitung Mainz-Rheinhessen | 28.06.2022 | Seite 8

Allgemeine Zeitung Alzey | 28.06.2022 | Seite 8

Allgemeine Zeitung Bad Kreuznach | 28.06.2022 | Seite 8

Allgemeine Zeitung Ingelheim-Bingen | 28.06.2022 | Seite 8

Rüsselsheimer Echo | 28.06.2022 | Seite 8

Bürstädter Zeitung | 28.06.2022 | Seite 8

Darmstädter Echo (Hauptausgabe) | 28.06.2022 | Seite 8

Groß-Gerauer Echo | 28.06.2022 | Seite 8

Odenwälder Echo | 28.06.2022 | Seite 8

Starkenburger Echo | 28.06.2022 | Seite 8

Dill-Zeitung | 28.06.2022 | Seite 7

Lampertheimer Zeitung | 28.06.2022 | Seite 8

Lauterbacher Anzeiger | 28.06.2022 | Seite 7

Main-Spitze | 28.06.2022 | Seite 8

Oberhessische Zeitung (Hauptausgabe) | 28.06.2022 | Seite 7

Wetzlarer Neue Zeitung (Hauptausgabe) | 28.06.2022 | Seite 7

Herborner Tageblatt | 28.06.2022 | Seite 7

Hinterländer Anzeiger | 28.06.2022 | Seite 7

Weilburger Tageblatt | 28.06.2022 | Seite 7

Wiesbadener Kurier Stadtausgabe (Hauptausgabe) | 28.06.2022 | Seite 8

Wiesbadener Kurier - Rheingau-Kurier | 28.06.2022 | Seite 8

Wiesbadener Kurier - Untertaunus-Kurier / Aar-Bote | 28.06.2022 | Seite 8

Idsteiner Zeitung | 28.06.2022 | Seite 8

Wormser Zeitung | 28.06.2022 | Seite 8

TWEET VON trendreport_de:

5

Twitter / trendreport_de | 21.06.2022 | Online

Vernetzung ist Einfallstor für Hacker

Cybercrime: Wie der Wiesbadener Sicherheitsspezialist

Comforte AG die Zahlungsdaten von Bankkarten schützt

Von Karl Schlieker

WIESBADEN. Milliarden Schäden, geringe Aufklärungsquote. Die Cyberkriminalität wächst ungebrochen. Im vergangenen Jahr wurden nach dem Lagebericht des Bundeskriminalamts 146.000 Straftaten von Hackern und Computerbetrüggern registriert. Der Schaden summierte sich auf 223 Milliarden Euro. Das war mehr als doppelt so viel wie im Corona-Vorkrisenjahr 2019. Doch wie sollen Behörden und Unternehmen reagieren? Der Wiesbadener Sicherheitsspezialist Comforte favorisiert einen datenzentrierten Ansatz, auf den nach dessen Angaben bereits drei der fünf größten Kreditkartengesellschaften setzen. „Mehr als jede zweite Kartenzahlung weltweit wird von uns geschützt“, berichtet Vorstandschef Michael Deissner in Wiesbaden.

Angesichts der zunehmenden Vernetzung zwischen Vertriebs-, Produktions-, Zulieferbetrieben und Kunden sowie der Verlagerung von Funktionen in die Cloud nutzen die alten Schutzkonzepte nichts mehr. „Wie im Mittelalter bauten viele Unternehmen in der Vergangenheit möglichst hohe Burgmauern um die eigenen Rechner im Keller“, berichtet Deissner im Gespräch

mit dieser Zeitung. Da die Firmendaten aber längst nicht mehr im eigenen Unternehmen bleiben, hätten sich die Angriffspunkte vervielfacht. Die Frage sei heute nicht mehr, wie häufig ein Unternehmen am Tag angegriffen wird, sondern wie oft Hacker erfolgreich sind. Ein Unternehmen wie Comforte werde beispielsweise 400 bis 600 Mal am Tag attackiert. „Das Problem sitzt oft vor dem Rechner. Es ist der unvorsichtige oder abgelenkte Mitarbeiter.“ Problematisch sei, dass ein Dateneinbruch oft erst Monate später bemerkt werde, wenn die Daten bereits verschlüsselt oder im Darknet veröffentlicht wurden. „Der Schaden ist immens.“ Die einmal gestohlenen Daten seien nicht rückholbar, wenn sie ins Netz gestellt wurden.

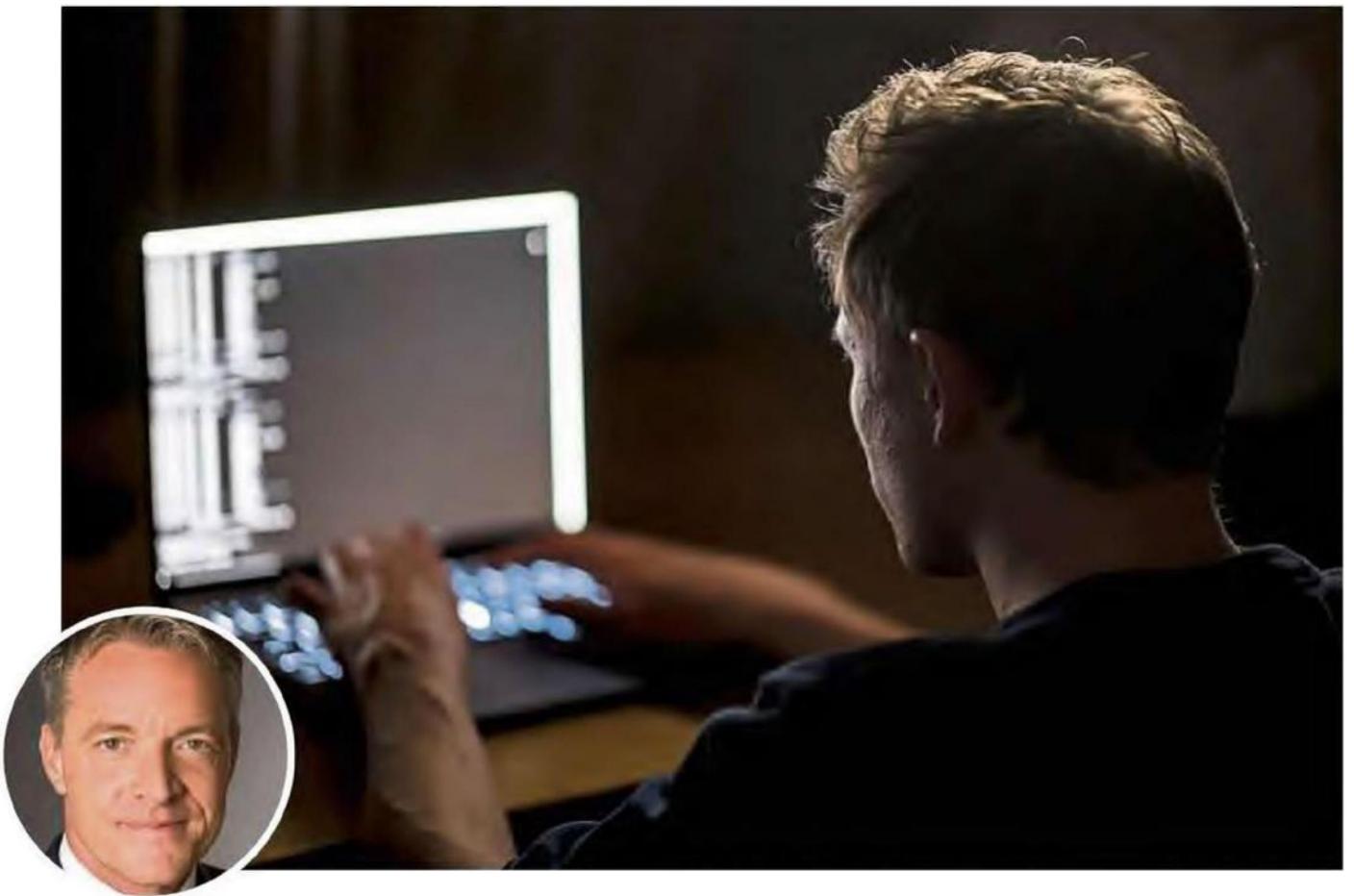
„Die Unternehmen stehen vor einer mehrfachen Herausforderung: Einerseits wollen sie sich vernetzen und mithilfe der Künstlichen Intelligenz große Datenmengen verarbeiten, andererseits müssen sie aber einen hohen möglichst effektiven Schutz der Daten verankern.“ Die klassischen Schutzkonzepte, die die Daten weitgehend isolieren, widersprechen diesen Zielen, da damit automatisierte Geschäftsprozesse und Datenanalysen eingeschränkt werden. Der Wiesbadener Sicher-

heitsspezialist Comforte setzt dagegen auf eine sogenannte datenzentrierte Sicherheit, mit der sensible Daten geschützt, kontrolliert, geprüft und trotzdem weiter bearbeitet werden können. Der Clou: Die Daten werden durch Token ersetzt, wobei das ursprüngliche Datenformat erhalten bleibt. Die 16 Stellen der Kreditkartennummern werden dabei beispielsweise durch einen Comforte-Algorithmus in eine komplett neue Zahlenfolge mit 16 Stellen übersetzt. Dabei ist für Außenstehende nicht erkennbar, dass es sich um eine komplett neue Nummer handelt. Der Platzhalter in Form eines Tokens könne dann mit der Comforte-Lösung wieder zurückübersetzt werden. Wenn das Unternehmen die exakten Ursprungsdaten benötigt, kann es sie mit einem Schlüssel öffnen.

„Großer Vorteil des Konzepts: Selbst wenn Daten auf dem Weg vom Einzelhändler zum Kreditkartenanbieter abgegriffen werden sollten, kann niemand etwas mit den Platzhalter-Daten anfangen.“ Man müsste den patentgeschützten Comforte-Algorithmus knacken, um die Daten zu übersetzen und nutzen zu können. Dafür müssten die Hacker aber merken, dass die Daten nicht korrekt seien.

Zwei der weltweit größten Einzelhändler sind Kunden

Neben den drei großen Kreditkartenanbietern zählen laut Deissner zwei der weltweit größten Einzelhändler sowie 27 weltweit operierende Großbanken zu den Comforte-Kunden. Das Unternehmen wurde 1998 von Entwicklern einer Vernetzungslösung für unternehmenskritische Systeme gegründet. „Der nächste logische Schritt war, nicht nur die Unternehmen zu vernetzen, sondern auch die Kommunikation zu sichern“, berichtet der ehemalige SAP-Manager Deissner, der 2016 bei Comforte einstieg. Bisher haben die Wiesbadener mit 150 Mitarbeitenden vor allem Kunden in Amerika. US-Kreditkartengesellschaften, Großbanken und Einzelhändler steuern rund zwei Drittel zum Umsatz von 30 Millionen Euro bei. Weitere 20 Prozent der Umsätze stammen aus Übersee. Lediglich rund zehn Prozent der Erlöse erzielt Comforte bisher in Europa. Nun soll auch der Heimatmarkt Deutschland intensiver beachtet werden. Schließlich ist nach Deissners Überzeugung sinnvoll, dass heimische Anbieter eine von US-Konzernen unabhängige Cybersicherheitsarchitektur zusehen können.



Angriffspunkte für Hacker haben sich laut Comferte-Chef Michael Deissner vervielfacht.

Fotos: dpa / Comferte