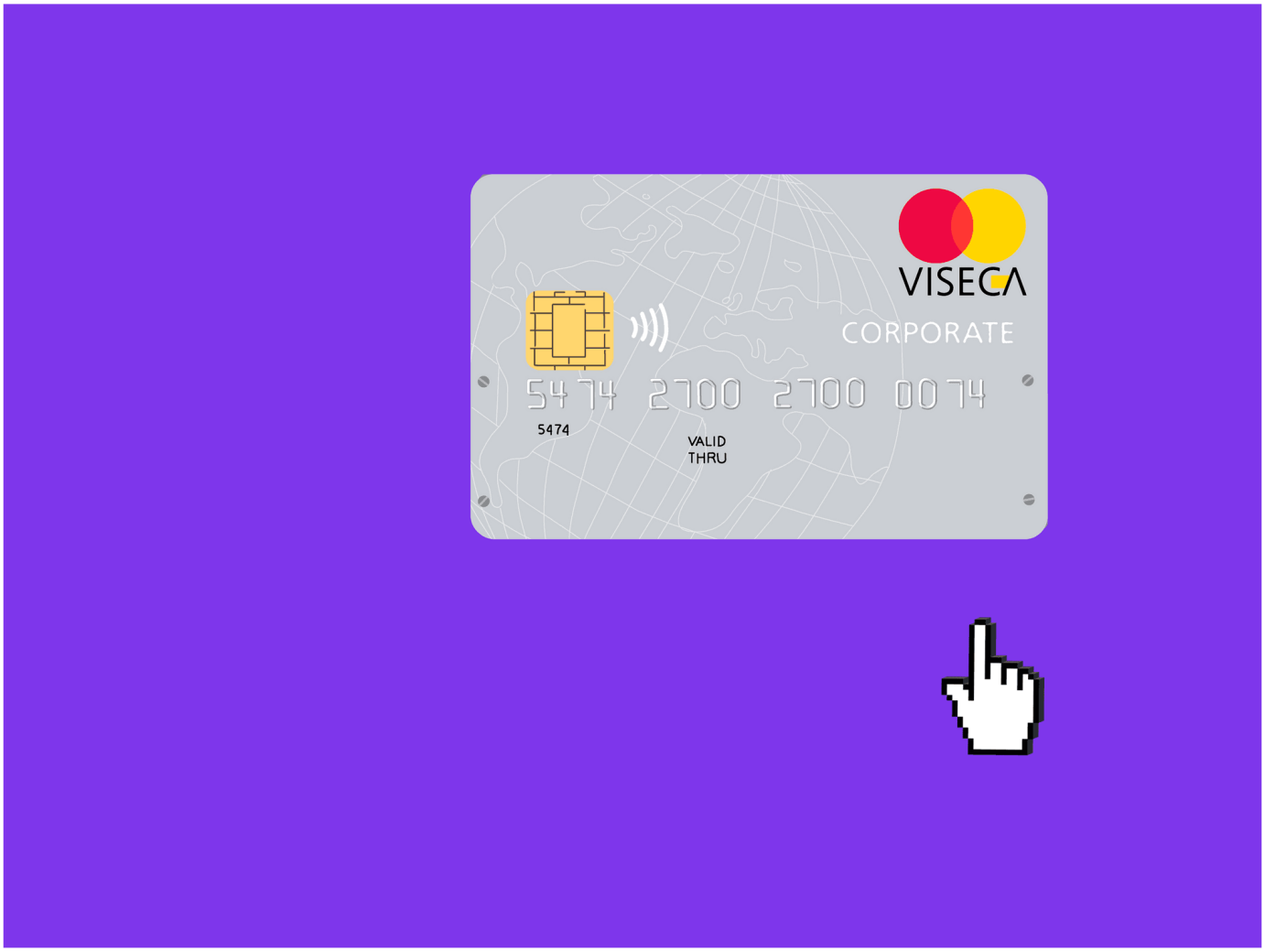


Zehntausende Schweizer Kreditkarten-Abrechnungen offen zugänglich im Internet

Wegen eines Lecks bei Viseca waren Abbuchungen von Firmenkunden online einsehbar. Der Schweizer Finanzdienstleister unterliess es, alle betroffenen Kunden zu informieren.

Eine Recherche von Adrienne Fichter (Text) und Alexander Glandien (Illustration), 20.03.2023

Abbuchungen für Google Cloud, Belege für Beschaffungen beim Elektrohändler, Rechnungen für Treffen mit Stammkundinnen in Cafés: Das sind Firmendaten, die nicht für die Öffentlichkeit bestimmt sind.

Doch genau solche Kreditkartendaten von Zehntausenden KMU-Kunden des Schweizer Finanzdienstleisters Viseca waren während 18 Monaten frei im Internet zugänglich und für alle einsehbar.

Viseca ist nicht irgendein Unternehmen: Sie verwaltet die Kreditkarten aller Kantonalbanken, der Raiffeisen-Gruppe, der Bank Cler sowie von Regional-, Privat- und Handelsbanken. Damit gehört sie zu den sechs grössten Schweizer Kreditkartenanbietern.

Entdeckt hat die Sicherheitslücke im digitalen Kundenportal von Viseca die IT-Sicherheitsfirma Pentagrid. Sie wandte sich mit ihren Informationen zunächst an den Finanzdienstleister und danach an die Republik. Aktuelle Recherchen belegen, dass das Datenleck sämtliche KMU mit einer Viseca-Kreditkarte umfasst. Inzwischen hat die Kreditkartenfirma das Leck gestopft.

Doch es bleiben Fragen: Was ist da genau passiert? Wie ist ein solcher Fehler überhaupt möglich? Und welche Folgen haben solche Sicherheitslücken?

Die wichtigsten Aspekte des Viseca-Falls in 10 Fragen und Antworten:

1. Die Sicherheitslücke: Worum geht es?

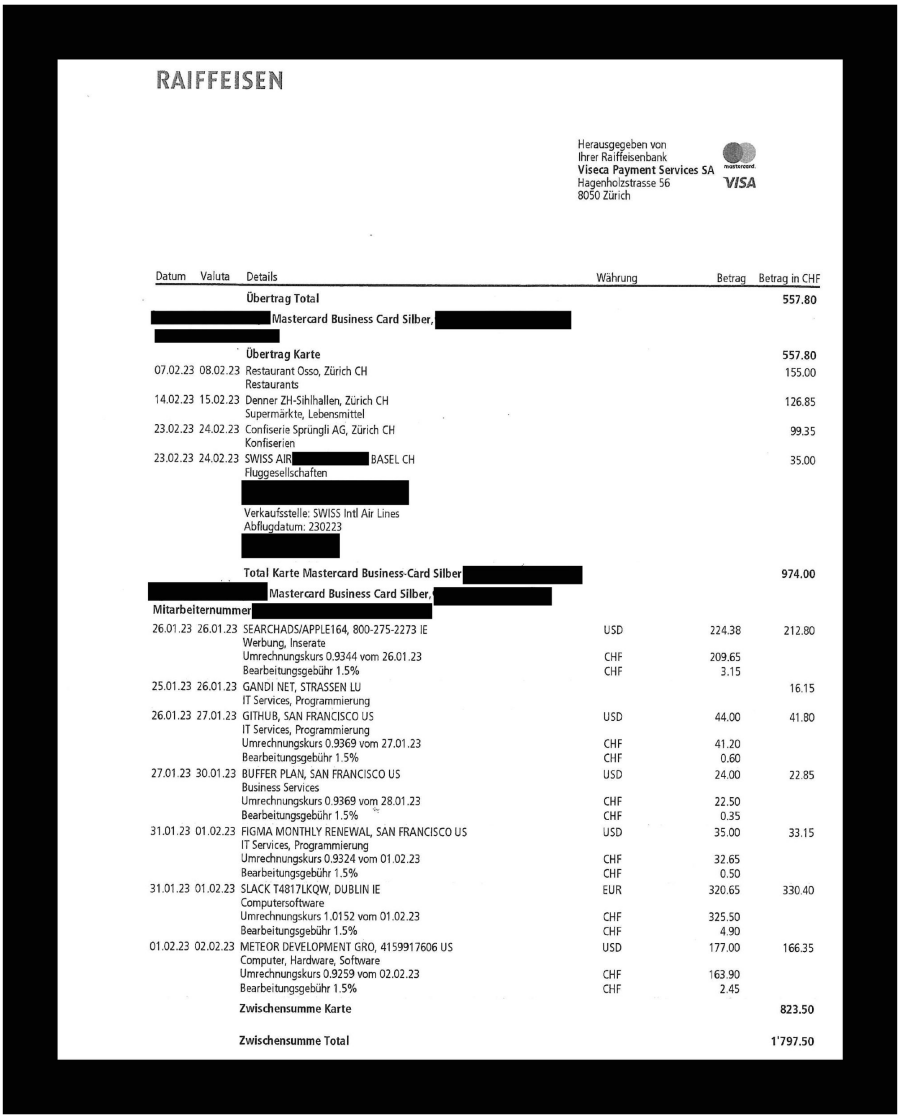
Zwischen Juni 2021 und November 2022 waren die monatlichen Kreditkartenabrechnungen von Zehntausenden Viseca-Geschäftskunden frei im Internet zugänglich – wie in einem Telefonbuch. Das ist durchaus wörtlich gemeint: Für den Zugriff auf die Daten waren kaum technische Kenntnisse nötig. Das Einzige, was man brauchte, um an die Daten zu kommen, war ein funktionierender Browser.

2. Die Daten: Was war frei im Internet verfügbar?

Die gefundenen Informationen waren höchst vertraulich. Aus den Abrechnungen liess sich herauslesen, welche Unternehmen wann wo was einkauften oder in welcher Cloud sie ihre Daten speicherten. Hätte jemand die Daten massenhaft aus dem Internet heruntergeladen, wären einige der Geschäftsbeziehungen der Firmen vollständig rekonstruierbar gewesen.

Konkret enthielten die Abrechnungen die Firmenadresse, die Kartenkontonummer, die Namen aller Karteninhaber (Geschäftsführerinnen, aber auch leitende Angestellte), eine maskierte Form der Kreditkartennummer (also zum Beispiel 1111 11XX XXXX 1111), die Kartenlimite, den Kartentyp – und den Namen der Bank des Unternehmens. Das ritzte auch das Bankkundengeheimnis. Ausserdem waren teilweise konkrete Transaktionen erkennbar und auch, wer sie durchführte.

Viseca-Sprecher Nicolas Kucera weist darauf hin, dass die hinterlegten PDF-Abrechnungen nach 13 Monaten jeweils gelöscht würden.



RAIFFEISEN

Herausgegeben von
Ihrer Raiffeisenbank
Viseca Payment Services SA
Hagenholzstrasse 56
8050 Zürich

Datum	Valuta	Details	Währung	Betrag	Betrag in CHF
		Übertrag Total			**557.80**
[redacted]		**Mastercard Business Card Silber,** [redacted]			
		Übertrag Karte			**557.80**
07.02.23	08.02.23	Restaurant Osso, Zürich CH Restaurants			155.00
14.02.23	15.02.23	Denner ZH-Sihlhallen, Zürich CH Supermärkte, Lebensmittel			126.85
23.02.23	24.02.23	Confiserie Sprüngli AG, Zürich CH Konfiserien			99.35
23.02.23	24.02.23	SWISS AIR [redacted] BASEL CH Fluggesellschaften			35.00
		[redacted] Verkaufsstelle: SWISS Intl Air Lines Abflugdatum: 230223 [redacted]			
		Total Karte Mastercard Business-Card Silber [redacted]			**974.00**
[redacted]		**Mastercard Business Card Silber,** [redacted]			
Mitarbeiternummer [redacted]					
26.01.23	26.01.23	SEARCHADS/APPLE164, 800-275-2273 IE Werbung, Inserate	USD	224.38	212.80
		Umrechnungskurs 0.9344 vom 26.01.23	CHF	209.65	
		Bearbeitungsgebühr 1.5%	CHF	3.15	
25.01.23	26.01.23	GANDI NET, STRASSEN LU IT Services, Programmierung			16.15
26.01.23	27.01.23	GITHUB, SAN FRANCISCO US IT Services, Programmierung	USD	44.00	41.80
		Umrechnungskurs 0.9369 vom 27.01.23	CHF	41.20	
		Bearbeitungsgebühr 1.5%	CHF	0.60	
27.01.23	30.01.23	BUFFER PLAN, SAN FRANCISCO US Business Services	USD	24.00	22.85
		Umrechnungskurs 0.9369 vom 28.01.23	CHF	22.50	
		Bearbeitungsgebühr 1.5%	CHF	0.35	
31.01.23	01.02.23	FIGMA MONTHLY RENEWAL, SAN FRANCISCO US IT Services, Programmierung	USD	35.00	33.15
		Umrechnungskurs 0.9324 vom 01.02.23	CHF	32.65	
		Bearbeitungsgebühr 1.5%	CHF	0.50	
31.01.23	01.02.23	SLACK T4817LKQW, DUBLIN IE Computersoftware	EUR	320.65	330.40
		Umrechnungskurs 1.0152 vom 01.02.23	CHF	325.50	
		Bearbeitungsgebühr 1.5%	CHF	4.90	
01.02.23	02.02.23	METEOR DEVELOPMENT GRO, 4159917606 US Computer, Hardware, Software	USD	177.00	166.35
		Umrechnungskurs 0.9259 vom 02.02.23	CHF	163.90	
		Bearbeitungsgebühr 1.5%	CHF	2.45	
		Zwischensumme Karte			**823.50**
		Zwischensumme Total			**1'797.50**

Unter den frei einsehbaren Abrechnungen befanden sich auch solche der Republik, im Original ohne geschwärzte Stellen. Diese haben wir aus Gründen des Persönlichkeitsschutzes hinzugefügt.

3. Das Ausmass: Wer ist vom Datenleck betroffen?

Betroffen waren alle KMU-Kunden, die beim Finanzdienstleister Viseca eine Kreditkarte haben. Der Marktanteil von Viseca bei Firmenkreditkarten beträgt laut Branchenkennern rund 25 Prozent. «Viele Firmenkunden dürften eine Karte der Kantonalbank nutzen», sagt Ralf Beyeler vom Vergleichsdienst Moneyland dazu.

Konfrontiert mit den Recherchen zum Sicherheitsleck, räumt Viseca ein, dass durch ein Datenleck die Kreditkarteninformationen aller KMU-Kundinnen offen im Netz lagen. Sprecher Nicolas Kucera sagt dazu: «Es sind potenziell die Businesskunden betroffen.» In den Antworten suggeriert Viseca aber zunächst, dass es sich dabei nur um Nutzerinnen des Spesenmanagement-Tools «eXpense» handelte. Eine genaue Zahl wollte das Unternehmen aus Gründen der Wahrung des Geschäftsgeheimnisses nicht nennen.

Weitere Recherchen der Republik brachten allerdings ans Licht, dass diese Antwort – zumindest technisch gesehen – nicht korrekt war. Denn auch die Abrechnungen der KMU ohne «eXpense»-Konto waren öffentlich zugänglich (siehe Infobox «Wie wir das Ausmass des Datenlecks eruiert ha-

ben»). Das bedeutet, dass die Kreditkartenabrechnungen von Zehntausenden Schweizer Firmen im Internet einsehbar waren. Darunter befanden sich übrigens auch Abrechnungen der Republik, wie sich während der Recherchen zeigte.

Ich will es genauer wissen: Wie wir das Ausmass des Datenlecks eruiert haben

Viseca suggerierte zunächst, dass nur ein bestimmter Teil ihrer Kunden betroffen gewesen sei, nämlich jene, die ein Tool namens «eXpense» verwendeten.

Recherchen der Republik zeigen jedoch, dass das Datenleck über die beschriebene Kundengruppe hinausgeht. Wir gelangten an verschiedene Kreditkartenabrechnungen von drei Firmen aus der Gastroindustrie. Und fragten bei den Geschäftsführern dieser Firmen nach, ob sie «eXpense» kennten und dort ein Benutzerkonto eingerichtet hätten.

Alle drei Firmen, die anonym bleiben wollen, antworteten mit Nein.

Damit wurde klar: Nicht nur «eXpense»-Nutzerinnen waren von der Lücke betroffen, sondern ein grosser Teil der Firmen mit einer Viseca-Kreditkarte.

Wie ist das möglich? Wenn bei «eXpense» eine Kreditkartenabrechnung einer Firma abgerufen wird, «holt» das Tool diese Daten beim Kreditkartenherausgeber. Das Testkonto des Spesenmanagement-Tools dient damit als «Eintrittsticket» für Unbefugte. Mit dieser gültigen URL im Browser kann man sich einfach «durchprobieren», bis man auf ein PDF einer Kreditkartenabrechnung stösst.

4. Die Aufdeckung: Wie wurde das Leck entdeckt?

Durch Zufall. «Am Anfang war es bloss ein mulmiges Gefühl», sagt Tobias Ospelt, Mitgründer von Pentagrid. Seine Firma benötigte ein Spesentool, um Abrechnungen digital zu verwalten. Und Viseca bietet mit «eXpense» genau ein solches Werkzeug an. Ospelt wollte dieses ausprobieren, legte ein Benutzerkonto für Pentagrid an – und wurde misstrauisch.

Aus seiner Sicht wurden im Anmeldeprozess gängige Sicherheitsstandards nicht erfüllt. Statt dass wie üblich für die 2-Faktor-Authentifizierung ein zufälliger Code generiert und den Nutzerinnen per SMS zugeschickt wird, nutzte Viseca für die Authentifizierung die letzten vier Ziffern der Telefonnummer des Nutzers. Eine fixe Zahlenreihe also, die durchaus auch von Dritten in Erfahrung gebracht werden kann.

5. Der Zugriff: Wie einfach war es, an die Kreditkarten-Daten zu gelangen?

Der «Bad Practice»-Fund im Anmeldeprozess von Viseca weckte den Instinkt von Tobias Ospelt, der seit über einem Jahrzehnt in der IT-Sicherheitsbranche arbeitet. Er beschloss, das Spesentool mit Kollegen genauer anzuschauen. Und er wusste, wo er ansetzen musste: bei der Funktion zum Herunterladen von PDF-Auszügen. Das sei ein Klassiker unter den Sicherheitslecks, sagt er. Gemäss seiner Erfahrung werde oft nicht richtig geprüft, ob ein Benutzer befugt ist, auf das entsprechende PDF zuzugreifen.

Und siehe da: Ospelt wurde nicht enttäuscht. Innert kurzer Zeit gelangten er und seine Kollegen an Kreditkartenabrechnungen, die nicht für sie bestimmt waren, und zwar durch das blosse Verändern einer Zahl in der Webadresse des Browsers.

Wie war das möglich? Konkret nutzten Ospelt und sein Team das Testkonto von «eXpense». Dabei handelt es sich um ein Standard-Benutzerkonto mit voreingestellten Testdaten. So können potenzielle Kundinnen die Vorzüge des Spesenmanagement-Tools ausprobieren. Wer sich einloggte, war gewissermassen ein normaler Viseca-Kunde, der sich im Dashboard Beispielrechnungen anschauen konnte. Bis zu diesem Punkt war noch alles im grünen Bereich.

Doch die Pentagrid-Experten hatten den Verdacht, dass sie womöglich noch mehr zu sehen bekommen könnten. Die URL des Browsers zeigte die Karten-ID des Testkontos und auch Abrechnungsnummern an. War es vielleicht möglich, durch die Änderung von einigen Ziffern in der Test-URL an die Daten ihres eigenen, inzwischen eingerichteten «eXpense»-Kontos zu kommen?

Auch hier bestätigte sich: Ja, das funktionierte. Angemeldet im Testkonto, konnte das Pentagrid-Team eine ihrer eigenen monatlichen Kreditkartenabrechnungen herunterladen. Die Sicherheitsexperten waren geschockt. Sie meldeten Viseca die Sicherheitslücke – und kontaktierten später die Republik.

6. Der zweite Test: War tatsächlich alles noch einfacher?

Die Republik führte einen zweiten Test durch. Wir wollten wissen, ob der Zugriff auch funktioniert, wenn man nicht im Viseca-Kundenportal «eXpense» eingeloggt ist. Zu diesem Zweck kopierten wir die URL des Testkontos in einen anderen Browser und veränderten die Ziffern am Ende der Zahlenreihe. Und tatsächlich: Es gab keine Einschränkungen. Die Republik hatte plötzlich Einsicht in Kreditkartenabrechnungen von drei fremden KMU.

Ich will es genauer wissen: Die Sicherheitslücke aus technischer Sicht

Die gefundenen Schwachstellen gehören laut Experten zu den Top-10-Sicherheitslücken und heissen im technischen Jargon *authentication failure* und *insecure direct object references (Idor)*.

Das heisst: Jede Internetnutzerin konnte «von aussen» dank Kenntnis der URL auf Daten zugreifen und brauchte weder technische Kenntnisse noch ein Log-in.

Noch gravierender als die fehlende Authentifizierung ist die fehlende Autorisierungskontrolle. Viseca hätte prüfen sollen, ob eine angemeldete Nutzerin überhaupt berechtigt ist, in der Webadresszeile eines Browsers jene Rechnungen abzurufen, die sie anfordert. Da gab es keine Einschränkungen bei den Zugriffsrechten.

Zum Problem führte ausserdem die durchschaubare Komposition einer gültigen URL: Diese setzte sich aus der Nummer der Karten-ID (wie in unserem Fall diejenige des Testkontos), dem Zeitstempel (Datum der Kreditkartenabrechnung) und sechs weiteren Ziffern zusammen. Die Republik brauchte

die URL manuell bloss dahingehend zu verändern, dass sie bei den letzten Ziffern einfach +1 rechnete (zum Beispiel «statementID456982» zu «statementID456983» machte), um so problemlos an die Kreditkartenrechnungen der drei erwähnten Firmen zu gelangen.

Den detaillierten technischen Bericht kann man im Blog der IT-Sicherheitsfirma Pentagrid nachlesen.

7. Der Schaden: Wurde die Sicherheitslücke ausgenutzt?

Viseca-Sprecher Nicolas Kucera sagt, dass ausser den «gemeldeten Zugriffen» (darunter diejenigen der Republik) in den entsprechenden Logdateien nichts verzeichnet sei. Das bedeutet: Nach Auskunft von Viseca gibt es keine Hinweise auf Hackerinnen.

Viseca liess zudem Expertinnen recherchieren, ob im Darknet Datensätze ihrer Kreditkartenkunden zum Verkauf angeboten werden. Auch da sei nichts auf dem Markt gefunden worden, sagt Kucera – was die Republik nach eigenen Recherchen bestätigen kann.

Zum heutigen Zeitpunkt ist davon auszugehen, dass die Lücke nicht von Unbefugten ausgenutzt worden ist.

8. Die Folgen: Muss die Sicherheitslücke den Behörden gemeldet werden?

Das ist unklar. Die Eidgenössische Finanzmarktaufsicht (Finma) sieht sich in diesem Fall als nicht zuständig an und verweist an den eidgenössischen Datenschutzbeauftragten (Edöb). Dessen Sprecherin Silvia Böhlen sagt auf Anfrage, es «besteht lediglich eine Meldepflicht, wenn die erfolgte Verletzung der Datensicherheit voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen kann».

Was ist ein hohes Risiko? Die Frage ist nicht leicht zu beantworten.

Die Daten aus den Kreditkartenabrechnungen hätten für Kriminelle durchaus interessant sein können. Zum Beispiel für die Erpressung von Firmeninhabern, die mit ihren Kreditkarten den Zugang zu einer Pornografie-Plattform bezahlten. Auch wären die gefundenen Informationen für Phishing-Kampagnen nützlich: «Ein mögliches hohes Risiko sehe ich darin, dass Angaben auf Kreditkartenrechnungen zum Teil für die Identifikation gegenüber dem Kundendienst eines beliebigen Services genutzt werden. Die Angaben könnten aber auch für Betrugsmaschen missbraucht werden», sagt Martin Steiger, IT-Anwalt und Mediensprecher der Digitalen Gesellschaft. Ausserdem erhalten Hackerinnen wissenswerte Informationen für künftige Cyberangriffe: wer in der Firma die Kreditkarte nutzt, wer die Lieferanten der Firma sind und wer die IT-Infrastruktur bereitstellt.

Derzeit scheint keine Bundesbehörde für solche Fälle zuständig zu sein – weshalb Viseca auch keine Sanktionen oder Bussen drohen.

Bei diesem Sicherheitsleck ist die Datensicherheit massiv vernachlässigt worden. Haben betroffene Firmen keine Möglichkeiten, dagegen vorzugehen? Doch, sagt IT-Anwalt Martin Steiger: «Unternehmen könnten unter dem noch geltenden Datenschutzgesetz Zivilklage erheben. Sie können eine widerrechtliche Persönlichkeitsverletzung feststellen lassen und al-

lenfalls Genugtuung oder Schadenersatz fordern.» Doch solche rechtlichen Schritte sind sehr aufwendig. Und es gebe, so Steiger, keine Erfolgsgarantie.

9. Die Reaktion: Wie reagierte Viseca auf das Leck?

Der IT-Sicherheitsexperte Tobias Ospelt meldete die Sicherheitslücke dem Kreditkartenanbieter am 11. November 2022. Dieser reagierte schnell: Knapp eine Woche später, also am 16. November 2022, war das Leck geschlossen. Viseca liess den Fall aufarbeiten und ihre Systeme nochmals umfassend prüfen.

Hier handelte die Kreditkartenfirma vorbildlich.

Anders sieht es mit der Information der Betroffenen zur Sicherheitslücke aus: Viseca informierte – angesichts der bevorstehenden Berichterstattung der Republik – in den letzten Wochen zwar die Banken und die drei Firmen, deren Daten die Republik zufällig bei ihren Tests gesehen hatte. Für die Kommunikation gegenüber den anderen Zehntausenden von Unternehmenskundinnen fühlt sich die Kreditkartenherausgeberin nicht verantwortlich. Viseca sagt, die Entscheidung über eine Information läge bei den Banken. Die Zürcher Kantonalbank nimmt keine Stellung und verweist auf Anfrage der Republik zurück an Viseca. Die Raiffeisen-Gruppe und die Bank Cler sehen von einer Information ab, weil bei ihren Firmenkundinnen kein unbefugter Zugriff geschehen sei.

Mit anderen Worten: Viele Betroffene und die Öffentlichkeit erfahren vom Sicherheitsleck bei Viseca wohl erst über diese Recherche.

10. Die Lehren: Warum hat Viseca das Sicherheitsleck nicht selbst bemerkt?

Das Spesenmanagement-Tool «eXpense» werde von einer externen Firma betrieben, hält Viseca in einem schriftlichen Statement fest. Dabei handelt es sich um Fiserv, eine global tätige US-Firma, die Technologien für den Finanzsektor anbietet.

Laut Viseca zeigte sich aufgrund einer technischen Analyse, dass die gemeldete Sicherheitslücke seit eineinhalb Jahren vorliegt.

Da es sich bei der gefundenen Lücke um eine klassische IT-Schwachstelle handelt, die bei jeder Sicherheitsprüfung als Erstes angeschaut wird, stellt sich die Frage, wie Viseca ihren technischen Zulieferer überhaupt prüfte. Und ob das entsprechende Tool je auf Angriffsszenarien getestet wurde. Viseca antwortet auf diese Frage bloss ausweichend: «Wir führen bei ‹eXpense› regelmässige automatisierte Sicherheitstests durch. Die absolute Fehlerfreiheit einer Anwendung kann aber nie mit absoluter Sicherheit bewiesen werden.»

Nachfrage: Wenn permanent getestet wird, wie konnte dann diese Schwachstelle so lange unbemerkt bleiben? Dazu sagt Sprecher Nicolas Kucera: «Grundsätzlich gehen wir davon aus, dass diese Sicherheitsschwäche deshalb unentdeckt blieb, da sie gemäss unseren Abklärungen zu keinem Zeitpunkt von irgendwelchen Dritten ausgenutzt wurde.»

Diese Antwort ist mehr als fragwürdig: Wenn Pentagrid sich nicht bei Viseca gemeldet und die Republik nicht weiterrecherchiert hätte, hätten die IT-Systeme vermutlich nie Alarm geschlagen. Es wäre möglich gewesen, in der entsprechenden URL – von Hand oder mit einem Programm – immer

wieder drei bis vier Ziffern zu ändern und höchstwahrscheinlich unentdeckt zu bleiben. Auf diesem Weg hätten die Daten auch heruntergeladen und eine Liste mit Abrechnungen angelegt werden können.

Dass ein solches Vorgehen machbar ist, hat Informatiker Simon Gantenbein schon in einer Republik-Recherche zum Onlinebanking von Postfinance aufgedeckt: Auch er konnte ungehindert eine Datenbank mit Postfinance-Kunden erstellen. Und knackte damit – zu Demonstrationszwecken – gleich das Bankgeheimnis.

Mit einem blauen Auge davongekommen

Cyberattacken zählen zu den Top-Risiken für den Finanzplatz Schweiz. Die Schweizer Banken widmen ihrer Abwehr deshalb seit längerem grosse Aufmerksamkeit, was sich auch in der Gründung eines eigenen Cybersicherheitszentrums zeigt.

Was ist das Fazit?

Viseca ist mit einem blauen Auge davongekommen. Zum einen, weil die Sicherheitslücke offenbar nicht ausgenutzt worden ist. Zum anderen, weil sich für den Fall keine Behörde zuständig fühlt und deshalb auch keine Sanktionen drohen.

Ganz anders präsentiert sich die Lage für die amerikanische Technologielieferantin Fiserv: Für sie könnte der Vorfall durchaus Folgen haben. Fiserv hat nämlich einen wichtigen Sicherheitsstandard für Kreditkartenzahlungen nicht erfüllt: den *Payment Card Industry Data Security Standard,* auch PCI DSS genannt. Eine Sanktion seitens der Branchenorganisation PCI SSC ist deshalb nicht auszuschliessen.

Viseca kommt nach diesem Datenleck weiter nicht zur Ruhe. Erst vor einem Monat wurde eine andere Datenschutzpanne beim Kreditkartenanbieter bekannt, die auf menschliches Versagen zurückzuführen ist. Eine Privatperson verlangte eine Datenauskunft bei Viseca. Ausgehändigt wurden ihr dann aus Versehen aber die Informationen zu einer anderen Person. Es handelte sich ausgerechnet um Martin Steiger, den erwähnten IT-Anwalt und Mediensprecher der Digitalen Gesellschaft. Dieser dokumentierte den Fall darauf öffentlich.