RSS
Rechtsservice- und Schlichtungsstelle
des Fachverbandes der Versicherungsmakler und
Berater in Versicherungsangelegenheiten

Stubenring 16 / Top 7
1010 Wien
Tel: 05 - 90 900 - DW 5085 (Fax DW 118225)
rss@wko.at

eine Einrichtung der
WKO WIRTSCHAFTSKAMMER ÖSTERREICH
Die Versicherungsmakler

RSS-0044-23-14
= RSS-E 116/23

Empfehlung der Schlichtungskommission vom 14.12.2023

Vorsitzender	Dr. Gerhard Hellwagner
Beratende Mitglieder	Marc Zickbauer Herbert Schmaranzer Dr. Hans Peer
Schriftführer	Mag. Christian Wetzelberger

Antragstellerin	*(anonymisiert)*	Versicherungs-nehmerin
vertreten durch	*(anonymisiert)*	Versicherungs-makler
Antragsgegnerin	1. *(anonymisiert)* 2. *(anonymisiert)* 3. *(anonymisiert)*	Versicherer
vertreten durch	*(anonymisiert)*	Versicherungs-makler

Spruch

Die Schlichtungskommission gibt keine Empfehlung ab.

Begründung

Die Antragstellerin hat einen Versicherungsvertrag über das Produkt „*(anonymisiert)* Cyber Pro+ Austria“ zur Versicherungsscheinnr. *(anonymisiert)* abgeschlossen. Als Vertragspartner und Risikoträger werden die drei Antragsgegnerinnen genannt, die Abwicklung des Versicherungsvertrages erfolgt durch die Antragsgegnerinnenvertreterin.

Das Produkt „*(anonymisiert)* Cyber Pro+ Austria“ enthält u.a. einen Versicherungsschutz für Cyberschäden und eine daraus resultierende Betriebsunterbrechung.

Auf Seite 8 des Versicherungsscheins heißt es unter den Punkten A5.4 und A5.4.1:

> *A5.4 Weitere Aspekte der Risikoerfassung*
> *1. Die IT des Unternehmens wird durch mindestens einen IT-Spezialisten betreut.*
> *Ja*

*2. Es werden regelmäßig (mind. wöchentlich) Datensicherungen durchgeführt. **
Ja
*3. Alle stationären und mobilen Arbeitsrechner sind mit aktueller Software zur Erkennung und Vermeidung von Schadsoftware ausgestattet. **
Ja
*4. Verfügbare Sicherheitsupdates werden ohne schuldhaftes Zögern durchgeführt, und für die Software, die für den Betrieb des IT-Systems erforderlich ist, werden lediglich Produkte eingesetzt, für die vom Hersteller Sicherheitsupdates bereitgestellt werden (dies betrifft v.a. Betriebssysteme, Virenscanner, Firewall, Router, NAS-Systeme). **
Ja
*5. Es existieren Regelungen zum Umgang mit IT-Zugangsdaten bei dem Versicherungsnehmer, deren Umsetzung überwacht wird. **
Ja
*6. Es werden Hard- und/oder Software (insbesondere Firewalls) zum Schutz des Unternehmensnetzwerks eingesetzt. **
Ja
*7. Mitarbeiter dürfen private Geräte für dienstliche Zwecke verwenden. * Ja*
8. Gab es in den letzten drei Jahren einen Cyberschaden oder einen Datenschutzvorfall im Unternehmen?
Nein
A5.4.1 Bedeutung für den Versicherungsschutz
1. Die vorstehenden Angaben des Versicherungsnehmers zu den konkreten IT-Sicherheitsmaßnahmen des Unternehmens werden Bestandteil des Versicherungsvertrages.
*2. Kein Versicherungsschutz besteht für Schäden, welche adäquat kausal auf eine fehlende IT-Sicherheitsmaßnahme zurückzuführen sind, nach welcher unter Ziffer 5.4 ausdrücklich gefragt worden ist. Von einem Fehlen einer IT-Sicherheitsmaßnahme ist bspw. auszugehen, wenn der Versicherungsnehmer eine oder mehrere der vorstehenden mit * markierten Fragen mit Nein beantwortet hat oder diese richtigerweise mit Nein hätte beantworten müssen, obwohl sie mit Ja beantwortet wurde(n). In letztem Fall behält sich der Versicherer einen Rücktritt vom Vertrag nach § 16 VersVG vor.*
Es besteht ebenfalls kein Versicherungsschutz für Schäden, welche adäquat kausal auf eine dienstliche Nutzung privater Geräte zurückzuführen ist, wenn und soweit der Versicherungsnehmer die vorstehende Risikofrage 7 mit Nein beantwortet hat.
Auf die gesonderte Mitteilung über die Folgen einer Verletzung der vorvertraglichen Anzeigepflicht nach § 16 VersVG wird bei der Übermittlung der Invitatio, also im Vorfeld des Vertragsschlusses, ausdrücklich hingewiesen.

Vereinbart sind die AVB *(anonymisiert)* Cyber Pro+ Austria 17.08.2020, welche auszugsweise lauten:

„(…) A1-9 Repräsentanten (A338)
1. Der Versicherungsnehmer muss sich die Kenntnis und das Verhalten seiner Repräsentanten (A338) zurechnen lassen.

2. Als Repräsentanten (A338), einschließlich Personen, die bei mitversicherten Unternehmen (A492) eine mit den vorgenannten Funktionen vergleichbare Funktion innehaben, gelten nur:
1. bei Aktiengesellschaften (AG): Die Mitglieder des Vorstandes
2. bei Gesellschaften mit beschränkter Haftung (GmbH): Die Geschäftsführer
3. bei Kommanditgesellschaften (KG): Die Komplementäre
4. bei offenen Handelsgesellschaften (OHG): Die Gesellschafter
5. bei Gesellschaften des bürgerlichen Rechts (GbR): Die Gesellschafter
6. bei Einzelfirmen: Die Inhaber
7. bei anderen Unternehmensformen (wie z.B. Genossenschaften, Verbände, Vereine, Körperschaften des öffentlichen Rechts, Kommunen, ausländische Unternehmen): Die nach dem Gesetz oder der Satzung berufenen obersten Vertretungsorgane.
(…)
B4-5 Anzuwendendes Recht
Für diesen Vertrag gilt österreichisches Recht. Es gelten insbesondere die Vorschriften des Versicherungsvertragsgesetzes (VersVG) sofern durch diesen Vertrag nichts Anderes geregelt wird.

Teil C – Besondere Versicherungsbedingungen
3 Schutz von Sachen und Daten - Folgen aus der Beeinträchtigung, Beschädigung oder Unbrauchbarmachung von Software und Daten
3.2 Folgen aus Erpressung
3.2.1 Versichert sind die notwendigen Kosten für Schadenmanagement (A487) durch die auf die Bearbeitung von Cyber-Versicherungsschäden spezialisierte und von den Risikoträgern dieses Versicherungsvertrages umfassend beauftragte (anonymisiert) im Falle von Erpressung (A130) einer in diesem Vertrag mitversicherten (A237) juristischen Person (A481), soweit dies das Ergebnis der Manipulation von Software oder Daten (A489) im Zusammenhang mit einer unbefugten Nutzung (A507) von IT-Systemen (A206) ist.

1.4.2 Versichert sind die notwendigen Kosten für die Schadenbearbeitung durch Experten (A516) nach Beauftragung durch die (anonymisiert) im Falle von Schäden infolge von Erpressung (A130) einer oder mehrerer in diesem Vertrag mitversicherte(n) (A237) juristische(n) Person(en) (A481) oder ihrer Repräsentanten (A338) im Einsatz für mitversicherte juristische Personen, soweit diese Erpressung das Ergebnis einer unbefugten Nutzung (A507) von IT-Systemen (A206) ist. Der Einsatz von Experten wird durch die (anonymisiert) beauftragt und gesteuert; er muss Aussicht auf Erfolg haben, dem Sachverhalt angemessen und wirtschaftlich sinnvoll sein.
3.2.2 Versichert sind die notwendigen Kosten für Experten (A516) nach Beauftragung durch die (anonymisiert) im Falle von Erpressung (A130) einer in diesem Vertrag mitversicherten (A237) juristischen Person (A481), soweit dies das Ergebnis der Manipulation von Software oder Daten (A489) im Zusammenhang mit einer unbefugten Nutzung (A507) von IT-Systemen (A206) ist. Der Einsatz von Experten wird durch die (anonymisiert) beauftragt und gesteuert; er muss Aussicht auf Erfolg haben, dem

Sachverhalt angemessen und wirtschaftlich sinnvoll sein. Die Regelungen dieser Klausel gewähren nicht eine Erstattung der im Rahmen einer Erpressung gezahlten Gelder oder Werte.
6 Betriebsunterbrechung - Folgen aus der Unterbrechung des Betriebes infolge eines versicherten Cyber-Schadenereignisses (…)
6.2 Folgen aus dem Ausfall von IT-Geräten (…)

Strittig ist die Deckung des folgenden Schadenfalles (Nr. *(anonymisiert)*). Die Schilderung ist – soweit unstrittig – dem Abschlussbericht der *(anonymisiert)* vom 24.8.2022 entnommen.

Am 25.01.2022 wurde die (anonymisiert) über einen möglichen IT-Sicherheitsvorfall bei der (anonymisiert) durch die (anonymisiert) informiert. Die (anonymisiert) wurde beauftragt den möglichen IT- Sicherheitsvorfall gemäß der Leistungsbeschreibung zu bearbeiten.
Der Ansprechpartner des Versicherungsnehmers Herr S(anonymisiert) ist am 25.01.2022 erfolgreich kontaktiert worden. (…)
Im Erstgespräch berichtete Herr S(anonymisiert), dass ein Großteil der Serversysteme inklusive der Backups von einem Verschlüsselungstrojaner verschlüsselt worden sind. So ließen sich Dateien nicht mehr öffnen und diese hatten die neue Dateiendung .elbie.
Gleichzeitig war im Dateinamen jeder verschlüsselten Datei eine ID sowie Kontaktadresse kodiert
Ebenso lag auf den verschlüsselten Systemen eine Erpressernachricht mit einer Zahlungsaufforderung zur Entschlüsselung der Daten (…).
2.3 Schadenursache
Die Artefakte der untersuchten Systeme deuten auf die offene RDP-Schnittstelle des Clients WEPC027 als Einfallstor hin.(…)
<u>Fazit</u>
Im vorliegenden Fall sind die IT-Systeme des Versicherungsnehmers (anonymisiert) mit einer Variante des Phobos Verschlüsselungstrojaners am Abend des 24.01.2022 verschlüsselt worden.
Das Einfallstor besteht mit hinreichend hoher Wahrscheinlichkeit in der RDP-Weiterleitung zum Client WEPC027. Auf diesem zeigten sich Spuren eines bestehenden Brute-Force-Angriffs. So zeigen sich im Zeitraum vom 25.01.2022 um 07:16:29 Uhr (UTC+1) bis 08:09:30 Uhr (UTC+1) insgesamt 12783 fehlgeschlagene externe Anmeldeversuche.
Nach aktuellem Kenntnisstand erfolgte der initiale Zugriff eines Angreifers zur IT-Infrastruktur am 16.01.2022 um 22:24:17 Uhr (UTC+1) über das Benutzerkonto wartung (SID: S-1-5-21-3704808591-536821595-3198812367-1261) auf den Client WEPC027. In den zur Verfügung gestellten Daten zeigt sich eine laterale Bewegung ausgehend vom Client WEPC027 ab dem 19.01.2022 01:59:29 Uhr (UTC+1).
Hinweise zu einem möglichen Datenabfluss konnten in den zur Verfügung gestellten Daten nicht nachgewiesen werden. Allerdings wurde ein Großteil von relevanten Daten zur Auswertung verschlüsselt, sodass eine fundierte Aussage nicht möglich ist.
5 Empfehlungen

Es wird empfohlen eine Neuinstallation von sämtlichen IT-Systemen empfohlen. Darüber hinaus können die Nutzdaten aus dem Backup, nach vorheriger Prüfung mit mehreren Antivirensystemen zurückgespielt werden. Gleichzeitig müssen sämtliche Kennwörter geändert werden.

Die mit einem Windows-Kennwort und dem Benutzernamen abgesicherte und eingerichtete RDP-Weiterleitung auf den Client entspricht nicht der gängigen Praxis zum Schutz dieser Schnittstelle. Es sollte mindestens ein entsprechend abgesichertes VPN genutzt und die RDP-Schnittstelle sollte nicht offen ins Internet exponiert werden."

Die Kosten für die Schadensfeststellung und Wiederherstellung der IT-Systeme belaufen sich auf € 242.987,05. Das Sachverständigenbüro *(anonymisiert)* wurde mit der Ermittlung des Betriebsunterbrechungsschadens beauftragt. An zusätzlichen Kosten der Schadensminderung wurde ein Aufwand von € 36.797,59 ermittelt, davon fallen € 5.515,66 unter den Selbstbehalt (6 Arbeitsstunden pro Mitarbeiter). Diese Beträge, in Summe € 274.268,98 brutto, wurden von Seiten der Antragsgegner bezahlt, 75% davon werden jedoch im Regressweg wiederum von der Antragstellerin eingefordert. Der Versicherungsfall sei grob fahrlässig herbeigeführt worden.

Dagegen richtet sich der Schlichtungsantrag vom 28.6.2023. Der Ausschlusstatbestand greife nur, wenn sich der Vorwurf grober Fahrlässigkeit gegen ein vertretungsbefugtes Organ der Antragstellerin, eines Vereines, richte. Auf einen Vorsatz oder ein grobes Verschulden eines IT-Spezialisten komme es nicht an.

Die Antragsgegnerinnenvertreterin nahm mit Schreiben vom 4.8.2023 wie folgt Stellung:

Im Rahmen des Vertragsabschlusses am 21.05.2021 hat unsere Versicherungsnehmerin unstreitig bestätigt, dass regelmäßige Sicherheitsupdates zeitnah durchgeführt werden und dass fachlich einschlägig ausgebildete Mitarbeiter die IT-Abteilung betreuen. Diese Zusicherungen war essenzielle Voraussetzung für den Abschluss dieses Cyber-Versicherungsvertrags.

Unsere Versicherungsnehmerin hat sich zur Sicherstellung dieser Vertragsvoraussetzung des Mitarbeiters S(anonymisiert) bedient. Unsere Versicherungsnehmerin ist verpflichtet, das ordnungsgemäße Einspielen von Sicherheitsupdates durch Ihren Mitarbeiter S(anonymisiert) zu überwachen. Es existieren weder ein schriftliche Weisungen, noch ein expliziter Patchmanagement- oder Berichtswesensprozess, noch ein Lasten- und Pflichtenheft der IT-Abteilung.

Nach aktueller Rechtsprechung ist unsere Versicherungsnehmerin zur Dokumentation ihrer Tätigkeiten verpflichtet. Auch diese ist im Rahmen der Schadenabwicklung nicht vorlegt worden.

Schadenursächlich war die offene RDP-Schnittstelle. Wäre diese geschlossen worden, so wäre der Inzident mit an Sicherheit grenzender Wahrscheinlichkeit verhindert worden. Hätte unsere Versicherungsnehmerin Ihre eigene IT-Abteilung ordnungsgemäß überwacht und instruiert, so wäre diese Sicherheitslücke aufgefallen und der Inzident verhindert worden.

In der fehlenden Überwachung der Tätigkeiten von Herrn S(anonymisiert) und mangelnden konkreten Weisungen liegen die Verursachungsbeiträge unserer Versicherungsnehmerin.
Unsere Versicherungsnehmerin ist Kauffrau und sich somit in besonderem Maße der Wichtigkeit ordnungsgemäßen Handelns bewusst.
Grob fahrlässig handelt, wer die im Verkehr erforderliche Sorgfalt in besonders schwerem Maß verletzt, schon einfachste, ganz naheliegende Überlegungen nicht anstellt und das nicht beachtet, was im konkreten Fall jedermann einsehen musste.
Dies setzt voraus, dass der Versicherungsnehmer wusste oder wissen musste, dass sein Verhalten geeignet war, den Eintritt des Versicherungsfalls oder die Vergrößerung des Schadens zu fördern. Es muss ihm klar sein, dass es ohne Weiteres nahelag, ein anderes Verhalten als das Tatsächliche zur Vermeidung des Versicherungsfalls in Betracht zu ziehen.
Dies führt bei Betrachtung aller objektiven Fakten zu einer im höchsten Maße grob fahrlässigen Herbeiführung des Versicherungsfalls gemäß § 61 AVersVG. Angesichts des Schweregrades des Verschuldens unser Versicherungsnehmerin ist eine Leistungskürzung von deutlich über 75 % berechtigt, wenn man die Wertungsmaßstäbe des deutschen VVGs zugrundlegt. Nach österreichischem Recht ist sogar eine gänzliche Leistungsverweigerung zulässig.

Die Antragstellervertreterin erstattete folgende Gegenäußerung:

„(…)Die Forderungen sind gänzlich unberechtigt, es mangelt bereits am Vorliegen wesentlicher Zurechnungskriterien, wie insbesondere rechtswidriges Verhalten bzw. dem Verschulden.
Das Vorbringen, dass die Antragstellerin bei Vertragsabschluss bestätigt hat, dass regelmäßig Sicherheitsupdates zeitnah durchgeführt werden und dass fachlich einschlägig ausgebildete Mitarbeiter die IT Abteilung betreuen, ist falsch und entspricht nicht den Gegebenheiten bei der Vertragsschließung.
Die Vertragsschließung erfolgte online im Büro der (anonymisiert) in Beisein und unter Mitwirkung des Maklerbetreuers der Antragsgegnerin.
Die allgemeinen Antragsfragen iSd vorvertraglichen Anzeigepflichten wurden online gestellt und befüllt.
Diese Angaben wurden zum integrierenden Bestandteil des Versicherungsvertrages und finden sich auf Seite 8 der Polizze.
In Pkt A5.4. auf Seite 8 der Polizze findet man unter Ziffer 1 die Frage nach Betreuung der IT des Unternehmens durch mindestens einen IT Spezialisten. Diese Frage wurde mit JA beantwortet.
In Pkt A5.4 und in weiteren Punkten der Polizze bzw des Antrages findet man keine Auflage auf einen einschlägig ausgebildeten IT Mitarbeiter.
Das Gewerbe "Dienstleistungen in der automatischen Datenverarbeitung und Informationstechnik" ist nach unserer Rechtslage ein freies Gewerbe und unterliegt keiner Regelmentierung.
Ein „IT-Spezialist“ ist eine generische Berufsbezeichnung, die meistens in folgender Job-Bezeichnung konkretisiert wird: „IT-Spezialist “.

Meistens ist diese Bezeichnung im Bereich der IT-Infrastruktur und Systemadministration anzutreffen, teilweise auch in der Softwareentwicklung oder IT-Beratung.
Daher kann der Aufgabenbereich des IT-Spezialisten nur schwer allgemeingültig eingegrenzt werden.
Für das Leben und Arbeiten als IT-Spezialist ist keine gesonderte Ausbildung erforderlich und sind auch in Großbetrieben wie bei Versicherungsunternehmen IT Spezialisten angelernte Mitarbeiter.
Der Mitarbeiter der Antragstellerin, Herr S(anonymisiert), ist für die „IT" des Unternehmens eingesetzt und gehört die Administration der IT zu seinen Aufgaben.
Sohin ist er ein „IT Spezialist" im Sinne obiger Definition.
In Ziffer 4. des Punktes A5.4 hat die Antragstellerin die Frage, dass verfügbare Sicherheitsupdates ohne schuldhaftes Zögern durchgeführt werden wahrheitsgemäß mit JA beantwortet.
Diese intransparente Frage setzt voraus, dass zum einem Sicherheitsupdates zur Verfügung stehen, wobei sich hier die Frage stellt, durch wen diese Updates zur Verfügung gestellt werden bzw. verfügbar, zum anderen, dass die Updates ohne schuldhafte Verzögerung eingespielt werden.
Keineswegs deckt sich dieser Punkt mit dem Vorbringen des Antraggegners, dass regelmäßige Sicherheitsupdates zeitnah durchgeführt werden müssen.
Weder bei den vorvertraglichen Anzeigepflichten noch bei den Obliegenheiten findet man eine Bestimmung, dass die Antragstellerin verpflichtet sei, das ordnungsgemäße Einspielen von Sicherheitsupdates durch ihren Mitarbeiter zu überwachen.
Weder bei den vorvertraglichen Anzeigepflichten noch bei den Obliegenheiten findet man eine Bestimmung, für das Vorliegen von schriftlichen Weisungen, expliziten Patchmanagement- oder Berichtswesensprozessen, sowie für das Vorliegen von Lasten- und Pflichtenhefte der IT-Abteilung.
Dieses Vorbringen der Antragsgegnerin ist lebensfremd, da für das Einspielen von vorgegebenen, sohin nicht selbst programmierten Sicherheitsupdates kein Pflichtenheft bzw. konkrete Weisungen erforderlich sind.
Sicherheitsupdates kann jeder Laie einspielen und wird regelmäßig im Privatbereich bei Verwendung von Stand- und Mobilgeräten gemacht.
Ein Geschäftsführer bzw Obfrau ist durchaus berechtigt, Aufgaben mit Ausnahme von Leitungsaufgaben zu delegieren.
Die Tätigkeit als IT Beauftragter ist keine Leitungsaufgabe und kann daher delegiert werden.
In analoger Anwendung der Business Judment Rules (§ 25 GmbHG) unterliegt die Geschäftsführung bzw Obfrauschaft einer angemessenen Informationsbasis.
So wird es im Normalfall wenig sinnvoll sein, sich über jedes Update im IT System zu informieren. Es genügt, wenn die in Frage kommende Person fachlich und persönlich geeignet ist.
Konsequenz der Leitungsfunktion des Geschäftsführers bzw Obfrau und seiner/ihrer grundsätzlichen Möglichkeit, Aufgaben im Unternehmen zu delegieren, ist die Verpflichtung zur Überwachung der nachgelagerten, ihm untergeordneten Mitarbeiter

Das Maß an erforderlicher Kontrolle orientiert sich dabei an verschiedenen Parametern:
Neben Art und Größe des von der Gesellschaft betriebenen Unternehmens sind vor allem auch dessen spezifische Risken zu berücksichtigen. (Vgl nur Spindler in MünchKomm AktG5 § 91 Rn 19.)
Auch die Umstände des Einzelfalls sind zu berücksichtigen: So bedürfen Mitarbeiter und Bereiche, in deren Rahmen es bereits zu Fehlern gekommen ist, einer engeren Überwachung als solche, wo das nicht der Fall ist.
Die (anonymisiert) ist die Serviceorganisation für alle (anonymisiert).
Diese Serviceorganisation besteht aus einer geringen Anzahl an Mitarbeitern (26 Mitarbeiter inkl.Obfrau und Stellvertretung, wobei die Mehrzahl der MA in der Buchhaltung und Lohnverrechnung zu finden sind) ohne Hierarchieebenen, sodass sich das Maß an Kontrolle reduziert.
Die Geschäftsführer bzw hier Obfrau hat einen entsprechenden Organisationsrahmen vorgegeben und ausreichend qualifizierte Angestellte bestellt, sodass sie sich grundsätzlich darauf verlassen, dass die Mitarbeiter den von ihnen zu verantwortenden Bereich sorgfaltsgemäß ausüben.
Die Geschäftsführung bzw Obfrau lässt sich regelmäßig über den jeweiligen Bereich berichten und schreitet ein, sobald ihr Unregelmäßigkeiten bekannt werden.
Sohin geht das Vorbringen der Antragstellerin ins Leere und ergibt sich dieses Vorbringen auch nicht aus unseren Rechtsvorschriften oder einschlägiger Judikatur.
Schlussendlich ist das Vorbringen grob fahrlässigen Verhaltens entschieden zurückzuweisen und geht in eine Schutzbehauptung der Antragstellerin, um die angefallenen Kosten rückverlangen zu können.
Die grobe Fahrlässigkeit ist von der Antragstellerin zu beweisen und dieser Beweis ist und wird ihr nicht gelingen.
Sollte sich jedoch herausstellen, dass entgegen unserer Rechtsmeinung und den vorliegenden Gegebenheiten eine Verantwortung der Antragstellerin gegeben ist, wird vorsorglich die Mitverantwortung der Antragsgegnerin infolge Mitwirkung an der Vertragsschließung durch ihren Maklerbetreuer eingewandt.“

Auf ein Vergleichsanbot der Antragsgegnerinnenvertreterin ging die Antragstellervertreterin nicht ein.

Rechtlich folgt:

Grob fahrlässig handelt, wer im täglichen Leben die erforderliche Sorgfalt gröblich, in hohem Grad, aus Unbekümmertheit oder Leichtfertigkeit außer acht lässt, wer nicht beachtet, was unter den gegebenen Umständen jedem einleuchten musste; grobe Fahrlässigkeit ist gegeben bei schlechthin unentschuldbaren Pflichtverletzungen, die das gewöhnliche Maß an nie ganz vermeidbaren Fahrlässigkeitshandlungen des täglichen Lebens ganz erheblich übersteigen (vgl RS0030303). Eine grobe Fahrlässigkeit ist nur dann anzunehmen, wenn eine auffallende und ungewöhnliche Sorglosigkeit vorliegt, wie sie nur bei besonders nachlässigen oder leichtsinnigen Menschen vorzukommen pflegt (vgl RS0030438).

Der Antragstellervertreterin ist dem Grunde nach zuzustimmen, dass ein Fehlverhalten des angestellten IT-Spezialisten der Antragstellerin nicht zuzurechnen ist. Die deutsche Repräsentantentheorie wird in der österreichischen Judikatur abgelehnt, dementsprechend wurde in den hier gegenständlichen AVB auch definiert, wessen Verhalten der Versicherungsnehmerin zuzurechnen ist.

Auch wenn der Versicherungsnehmer für solche Personen, die über diesen Personenkreis hinausgehen, daher nicht einstehen muss, kann ihn nach dem Selbstverschuldensprinzip ein zur Leistungsfreiheit des Versicherers führender Vorwurf treffen. Dies ist etwa dann der Fall, wenn es an der erforderlichen Sorgfalt in der Betriebsführung fehlt und der Betrieb demzufolge Organisationsmängel aufweist, die den Eintritt des Versicherungsfalles erheblich begünstigen (vgl RS0080407).

Wird der Risikoausschluss des § 61 VersVG behauptet, so muss der Versicherer auch die grobe Fahrlässigkeit des Versicherungsnehmers an der Herbeiführung des Versicherungsfalles beweisen (vgl RS0080378).

Die Antragsgegnervertreterin wirft der Antragstellerin ein Organisationsverschulden dahingehend vor, dass sie „weder ein schriftliche Weisungen (erteilt habe), noch ein expliziter Patchmanagement- oder Berichtswesensprozess, noch ein Lasten- und Pflichtenheft der IT-Abteilung“ existiere.

Soweit sich die Antragstellervertreterin darauf beruft, dass dazu in den Versicherungsbedingungen keine entsprechende vorvertragliche Anzeigepflicht oder Obliegenheit finde, ist ihr zu entgegnen, dass sich die Antragsgegnervertreterin eben nicht auf einen Verstoß gegen eine vorvertragliche Anzeigepflicht oder eine vorbeugende Obliegenheit beruft (diesfalls wäre bereits leichte Fahrlässigkeit deckungsschädlich), sondern explizit die grob fahrlässige Herbeiführung des Versicherungsfalles iSd § 61 VersVG einwendet.

Die Antragsgegnerin ist in diesem Zusammenhang nicht nur für das objektive Vorliegen eines Sorgfaltsverstoßes beweispflichtig, sondern auch für das subjektive Element. Weiters obliegt ihr der Beweis, dass der Sorgfaltsverstoß kausal für den Eintritt des Versicherungsfalles gewesen ist. Insgesamt bestreitet die Antragstellervertreterin einen Sorgfaltsverstoß der vertretungsbefugten Obfrau der Versicherungsnehmerin, da für die Tätigkeit als IT-Spezialist keine gesonderte Ausbildung notwendig sei und diese Tätigkeit regelmäßig angelernte Mitarbeiter übernehmen würden. Die Obfrau lasse sich regelmäßig über den jeweiligen Bereich berichten und schreite ein, sobald ihr Unregelmäßigkeiten bekannt würden. Mangels eines entsprechenden Anlasses konnte sie daher davon ausgehen, dass keine konkreten Weisungen erforderlich seien. Damit wird aber sowohl ein Fehlverhalten als auch implizit die Kausalität zwischen dem Verhalten der vertretungsbefugten Obfrau der Versicherungsnehmerin und dem Eintritt des Versicherungsfalles von der Antragstellervertreterin bestritten.

Gemäß Punkt 4.6.2. f) der Satzung kann keine Empfehlung abgegeben werden, wenn der Sachverhalt betreffend den Antragsgegenstand strittig ist und nur durch ein Beweisverfahren

nach den Zivilverfahrensgesetzen geklärt werden kann. In einem solchen Beweisverfahren läge es an der Antragsgegnerin, das konkrete Fehlverhalten der Obfrau samt dessen Kausalität für den Eintritt des Versicherungsfalles zu beweisen. Konkret bedeutet dies, dass zu prüfen sein wird, ob bei einer Beaufsichtigung der Mitarbeiter nach dem Maßstab einer ordentlichen Kauffrau derartige Handlungsanleitungen geschaffen worden wären, dass der Mitarbeiter die RDP-Schnittstelle als potentielle Angriffsquelle erkannt hätte und diese Schwachstelle geschlossen hätte.

Dabei wird zu berücksichtigen sein, dass die Obfrau selbst über keine Fachkenntnisse in IT-Angelegenheiten verfügen muss, sodass der Sorgfaltsmaßstab in subjektiver Hinsicht gegenüber dem eines IT-Spezialisten herabgesetzt ist.

Für die Schlichtungskommission:

Dr. Hellwagner eh.

Wien, am 14. Dezember 2023