Art Insurance Preventum

Cyber-Versicherung

Das Trojanische Pferd und die Ferse des Achilles

Warum nicht nur in antiken Sagen, sondern auch
im Zeitalter der Digitalisierung vor allem
die vermeintlich unsichtbaren Gefahren
Unternehmen verwundbar machen

Preventum
Treasure Your Art – Protect its Value
Individuelle Versicherungen für Teilnehmer im internationalen Kunstbetrieb

Preventum ist ein unabhängiger, international agierender Spezialversicherungsmakler. Wir beraten und betreuen Versicherungsnehmer aus unterschiedlichen Bereichen des Kunstmarktes. Zu unseren Kunden zählen vermögende Privatpersonen und Kunstsammler, Museen und Ausstellungshäuser, Kunststiftungen und Corporate Collections, Galerien und Kunstauktionshäuser sowie Unternehmen aus dem spezialisierten Finanzdienstleistungssektor.

Family Office Kultur
Unsere Family Office Kultur gewährleistet die umfassende, vertrauliche und persönliche Betreuung Ihrer Versicherungsbelange aus einer Hand.

Unabhängigkeit
Wir erschließen den Versicherungsmarkt in seiner vollen Breite und vertreten ausschließlich Ihre Interessen. Wir sind an keinen Versicherer gebunden, aber mit allen verbunden. So können wir Ihnen eine unabhängige Bestlösung für Ihren Bedarf garantieren.

Flexibilität
Mit Fachwissen in der Versicherungstechnik sowie Kunstexpertise und intimer Kenntnis des Kunstbetriebs entwickeln wir individuelle Konzepte unabhängig von standardisierten Produkten der Versicherer.

Ganzheitliche Beratung
Unser Engagement endet nicht mit der Betreuung Ihrer Versicherungsverträge. Wir bieten lösungsorientierte Beratung zum Risikomanagement von Kunst und sonstigen Wertgegenständen.

Umfassendes Verständnis
Kunstversicherung ist eng mit dem Kunstmarkt verknüpft. Die Versicherungswirtschaft unterliegt eigenen Gesetzen. Beide Welten erfolgreich zu verbinden, erfordert Kunstexpertise und versicherungstechnisches Know-how – wir bieten Ihnen beides.

Risikoszenarien durch zunehmende Digitalisierung

Digitales Arbeiten erleichtert und beschleunigt Prozesse und die Geschäftstätigkeit. Es macht uns flexibel und dadurch effizienter und zuverlässiger gegenüber unseren Kunden. Dabei unterschätzen wir, wie fragil und störanfällig digitale Strukturen sind.

Strenge Datenschutzverordnungen, ortsunabhängiges Arbeiten mit externen Geräten und Zugriff auf Unternehmensnetzwerke und Datenbanken in Cloud-Umgebung von unterwegs sowie die Zunahme von webbasierter Kommunikation und Transaktion erhöhen die Risiken der Manipulation und des Diebstahls von wertvollen und sensiblen Geschäftsdaten. Nicht nur allein die Kosten der Wiederherstellung und Wiedererlangung von Daten sind hier im Fokus. Der Kunstmarkt lebt von Reputation und Vertrauen. Ein Kontrollverlust ist daher umso schädlicher.

Während der erstmaligen Beschränkungen im Kontext der Covid-19 Pandemie arbeiteten rund 49% aller Beschäftigten ganz oder teilweise im Home Office. Rund 50% der Unternehmen geht davon aus, dass diese Arbeitsform auch nach der Pandemie weiter Bestand haben wird.

Das Arbeiten mit privaten Laptops und über Cloudumgebung und VPN-Zugriff auf das Unternehmensnetzwerk ist gleichbedeutend mit exponierten Risiken für Kundendaten und sämtliche Informationen, die in Ihrem IT-System gespeichert und abrufbar sind.

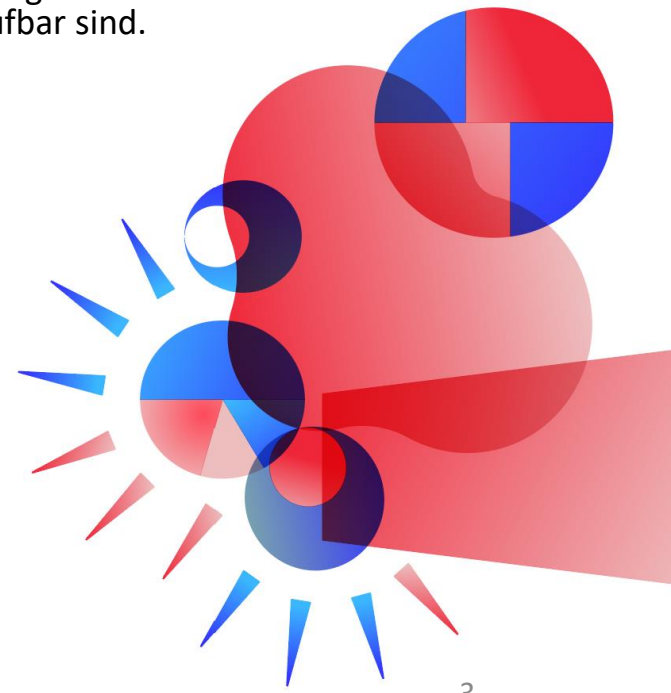
Die Nutzung von Video Chats ist seit Beginn der Pandemie drastisch gestiegen.
Die Sicherheitsstandards diverser Anbieter weisen jedoch nach wie vor Lücken auf.

Europol dokumentiert im jährlichen Bericht einen Anstieg von Cyberkriminalität in allen Bereichen im Zusammenhang mit der Covid-19 Pandemie.

Fast 70% aller deutschen Unternehmen und Institutionen wurden bereits Opfer eines Hackerangriffs.

Cyber-Angriffe gehen eher mit

- **Kosten für Datenwiederherstellung, mitunter auch Erpressungsgeldern**
- **Haftungsrisiken und Vertragsstrafen sowie Strafzahlungen bei Verstoß gegen Datenschutzverordnungen**
- **Reputationsverlust, Verlust des Kundenvertrauens**
- **Risiken für die Geschäftskontinuität**



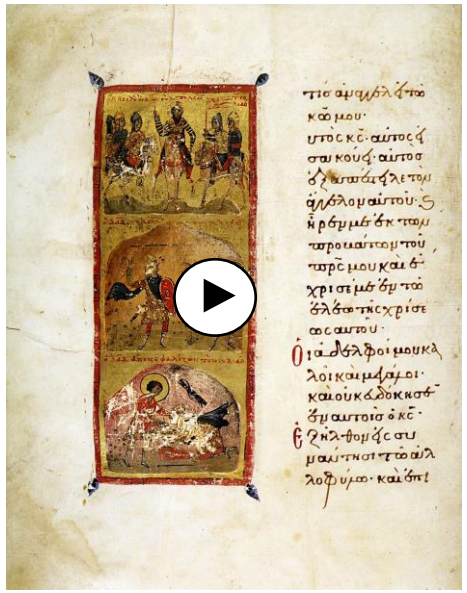
Gefahrenlage | Berichterstattung aus den Medien

Links zu den jeweiligen Artikeln hinterlegt, durch Klick auf die Abbildungen abrufbar

Zuletzt Opfer einer Phishing Attacke wurde die Londoner Galerie **Dickinson** im Zuge des Verkaufs eines Gemäldes von John Constable an das **Rijksmuseum in Enschede**. Der Rechtsstreit läuft bist heute. Das Rijksmuseum hatte von Dickinson eine digitale Rechnung erhalten. **Cyber-Kriminelle hatten den Email-Account von Dickinson gehackt** und unmittelbar auf den Rechnungsversand an das Rijksmuseum eine **fingierte Email mit neuen, abweichenden Zahlungsinstruktionen** gesandt. Das Gemälde befand sich bereits im Museum. Dickinson hat das Geld bis heute nicht erhalten. Das Museum weigert sich das Gemälde heraus zu geben. Immerhin wurden **3,0 Millionen USD** gezahlt.

Man-in-the-Middle Angriffe bei Galerien

Durch gehackte Mail-Accounts von Galerien wurden **Rechnungen über verkaufte Kunstwerke von Cyberkriminellen abgefangen und mit gefälschten Kontoverbindungen versendet.** Geschädigte waren die Galerien, die die Zahlung nicht erhielten und die Käufer, die weder die Kunstwerke, noch die fehlgeleitete Überweisung von ihren Banken zurückerhielten.



Im November 2020 wurde bekannt, dass die **Vatikanische Apostolische Bibliothek** seit Beginn ihres Digitalisierungsprojektes 2010 **vermehrt Opfer von Hackerangriffen ist, bis zu 100 Vorfälle je Monat**. Zum **Schutz der Datenbank** hat sich der Vatikan mit der Firma Darktrace zusammengetan, die **mittels Künstlicher Intelligenz** auch Plattformen wie ebay, T-Mobile und Samsung vor Angriffen schützt.

Über 1 ½ Jahre enthielt das **Käuferformular von Sotheby's Home einen schadhaften Code, der Kundeninformationen, darunter Kreditkarten-Nummern und CVV Codes, an unbekannte Dritte weitergab.**

Auch Christie's und Heritage Auctions wurden bereits Opfer von Hackerattacken.

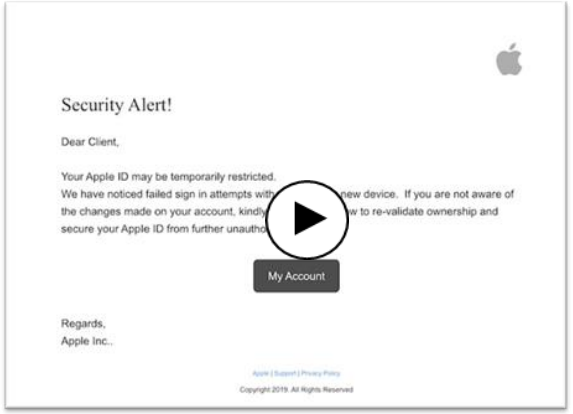
Gefahrenlage | Berichterstattung aus den Medien

Links zu den jeweiligen Artikeln hinterlegt, durch Klick auf die Abbildungen abrufbar

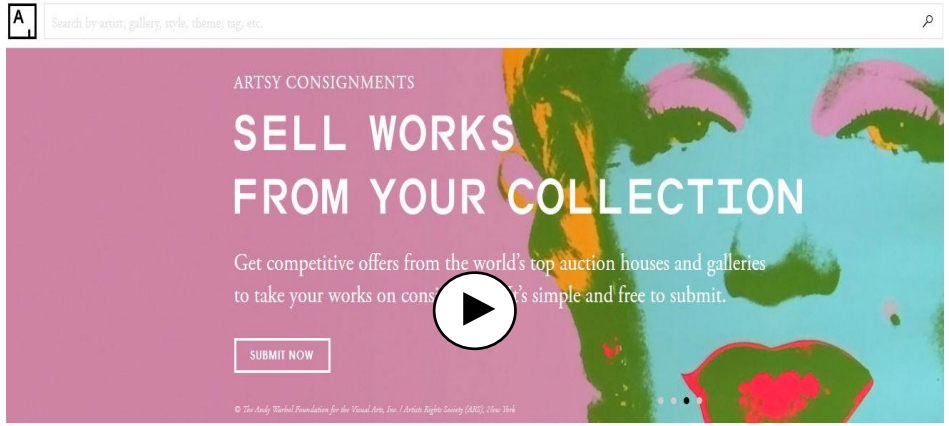
Im **Juni 2019** drangen **Hacker in das IT System des Juweliers Wempe** ein und infizierten es mit **Ransomware, die die gesamte IT verschlüsselte**.

Gegen die **Zahlung von EUR 1 Mio. Lösegeld in Bitcoins** erhielt das Unternehmen von den Erpressern ein Passwort, um wieder auf die Server und die Daten zugreifen zu können. Das Unternehmen musste externe Experten für IT-Forensik hinzuziehen und das LKA Hamburg sowie den Beauftragten für Datenschutz und Informationsfreiheit im Hamburger Senat involvieren.

Wempe implementierte mit externen IT-Experten ein neues IT-System und überarbeitete das Sicherheitskonzept in Zusammenarbeit mit Datenschützern.



Beispiel einer **Phishing-Mail aus dem 1. Quartal 2020** zum **Abfangen der Apple-Zugangsdaten**



1 Million Daten von Kunden der Kunstmarkt **Online-Plattform Artsy** wurden **2019 im Darknet zum Kauf angeboten.**

Cyber-Versicherung | Was ist versichert?

Eine Cyber-Versicherung deckt Kosten und Schadenbehebung bei Veränderung, Beschädigung, Zerstörung, Löschung, Verschlüsselung, Kopie oder Abhandenkommen von Daten unter anderem in Folge von:

- Netzwerksicherheitsverletzung
- (Hacker-)Angriffen – gezielt und ungezielt – auf das IT-System eines Versicherten
- Eingriffen in das IT-System des Versicherten zum Beispiel durch Phishing, d.h. die Beschaffung persönlicher Daten wie z.B. Passwörter, Kreditkartennummer o. Ä. mit gefälschten E-Mails oder Websites
- Schadprogrammen wie Viren, Würmern oder Trojanern, die sich im IT-System eines Versicherten ausbreiten und Daten verschlüsseln und zerstören bis hin zu einem kompletten System-Ausfall der IT
- Denial-of-Service-Angriffen, durch die der Betrieb des IT-Systems eines Versicherten unterbrochen und funktionsunfähig wird
- jeder Weitergabe von Schadprogrammen an das IT-System eines Dritten ausgehend von dem IT-System eines Versicherten
- Bedienfehlern
- einer Datenrechtsverletzung / Verstoß gegen gesetzliche und vertragliche Datenschutzbestimmungen sowie gegen Geheimhaltungspflichten (Cyber-Haftpflicht bei Drittschäden)
- einer Cyber-Erpressung
- Kosten für Aufrechterhaltung des Geschäftsbetriebs nach einer Cyberattacke und während der Wiederherstellung des IT-Systems
- eines Diebstahls mobiler Geräte, auf denen Kunden- und Geschäftsdaten gespeichert sind

Dabei werden neben Sofortmaßnahmen zur Beendigung eines Schadenszenarios auch weiterführende und beratende Maßnahmen nach einem Schadenfall durch den Versicherer übernommen.

Cyber-Versicherung | Präventive Maßnahmen als erste – Cyber-Versicherung als zweite Verteidigungslinie

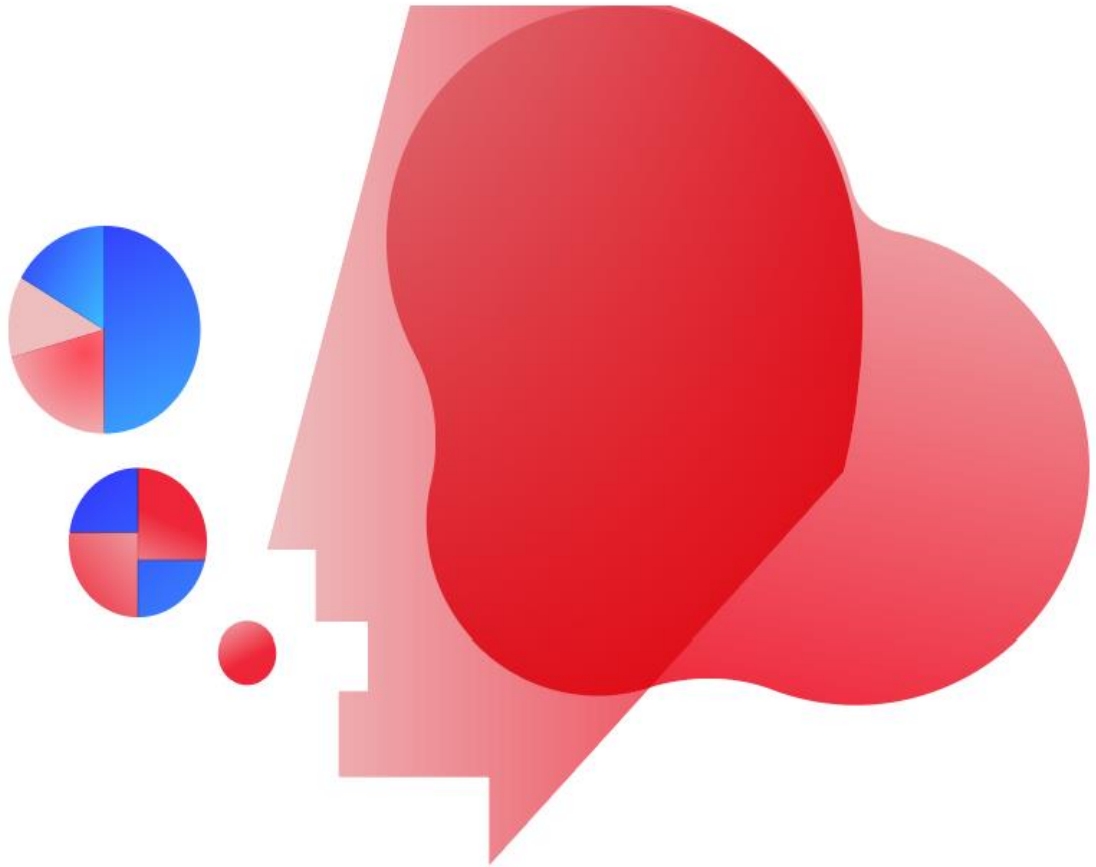
Prävention – Klassische Schutzmaßnahmen

Technische Maßnahmen

- Sicherung durch stets aktuellen Virenschutz und Firewall
- regelmäßiges Updaten der Systeme, um Sicherheitslücken zu schließen

Organisatorische & personelle Maßnahmen | Cyber-Risk Awareness Training:

- sichere Passwörter, sicherer Umgang mit mobilen Geräten
- Risikobewusstsein schulen, Schulung zu sicherem Umgang mit Daten, Erkennen von Phishing und schadhaften Inhalten
- Administrationsrechte einschränken
- keine Mehrfachnutzung von Konten
- regelmäßiges Monitoring und Informieren über aktuell kursierende Malware und Cyber-Kriminalität
- bei Transaktionen mit digitalem Rechnungsversand Kontodaten zusätzlich telefonisch verifizieren oder mit Passwort schützen



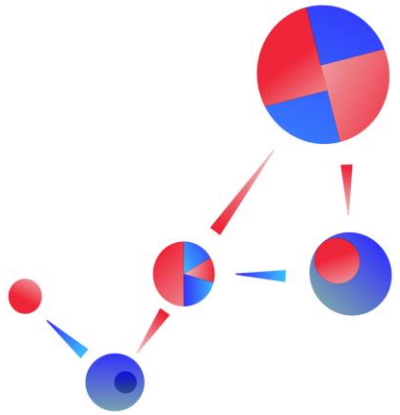
Versicherungsschutz – Risikotransfer

- Soforthilfe im Krisenfall
- Cyber-Eigenschäden
- Cyber-Haftpflicht
- Cyber-Betriebsunterbrechung

Cyber-Versicherung | Hilfe und Krisenmanagement im Schadenfall

Eine Cyber-Versicherung bietet im Schadenfall Soforthilfe durch IT-Spezialisten. In akuten Fällen wie einem Hacker-Angriff steht Ihnen eine 24h-Hotline zur Verfügung, die sofortigen technischen Support bietet.

Darüber hinaus erfolgt nicht nur die Kostenerstattung des entstandenen Schadens.



Eine Cyber-Versicherung ist eine Kombination aus

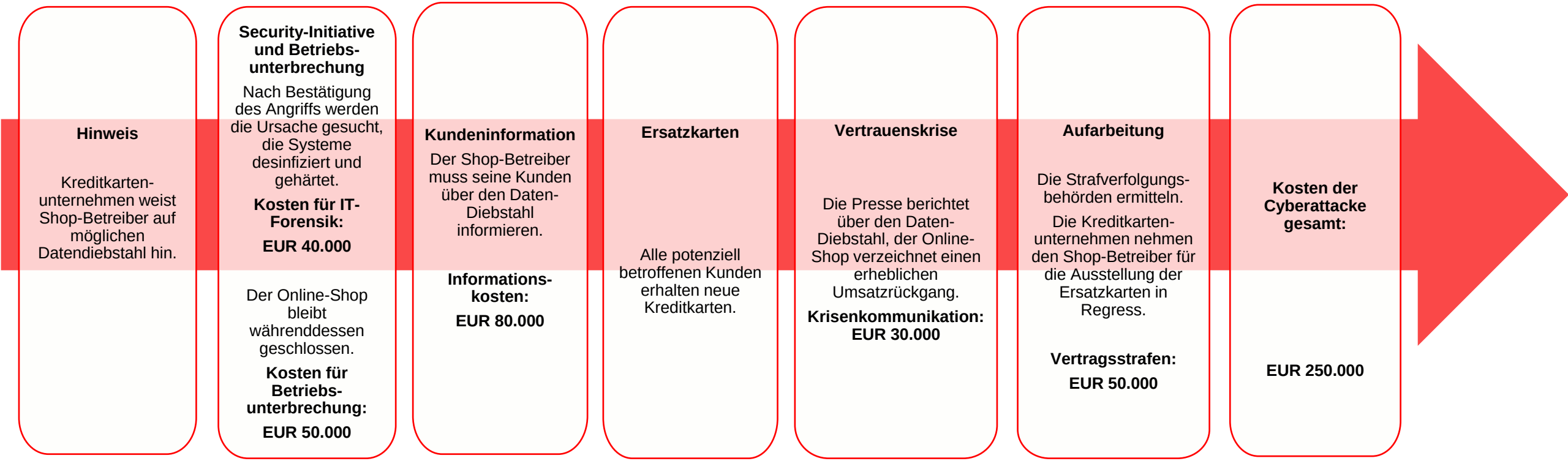
Die Cyber-Versicherung bietet umfangreiche Unterstützung bei der Bewältigung des Schadenszenarios durch ein engmaschiges Netzwerk von Datenschutzexperten, Datenforensikern und Krisenmanagern.

Sie steuern die weiteren Prozessen zur Daten- oder IT-System-Wiederherstellung sowie bei Datenschutzverletzungen zur Abwehr und Befriedigung von Schadenersatzansprüchen Dritter, d.h. von Kunden und Geschäftspartnern.

Cyber-Versicherung | Kosten im Schadenfall

Was eine Cyberattacke kosten kann und eine Cyber-Versicherung deckt

Musterszenario: Hacker erlangen Zugriff auf die Datenbank eines mittelständischen Online-Shops und stehlen die Kreditkarten-Daten von 50.000 Kunden



Quelle: GDV | Cyberrisiken im Mittelstand (2018)

Cyber-Versicherung | Kein Bedarf? Ein Irrtum denn…

Die meisten Unternehmen schätzen das Risiko einer Cyberattacke als gering ein.
„Wir sind zu klein – Wir sind nicht wichtig genug – Wir bewegen uns in einem Nischensegment“

Einige Gründe, die nahelegen die eigene Gefährdung durch Cyber-Risiken und den eigenen Bedarf nach einer Cyber-Versicherung zu prüfen

- Die IT-Abhängigkeit hat mit der zunehmenden Digitalisierung signifikant zugenommen, auch bei im Kunstmarkt und im Kunstbetrieb tätigen Unternehmen und Stiftungen. Ohne IT-System und vollumfänglichen Zugriff hierauf kann die Tätigkeit nicht ausgeübt werden.
- Oft gibt es keine eigene IT-Sicherheitsabteilung. Darüber hinaus fehlt bei Cyber-Attacken häufig das notwendige Netzwerk zu spezialisierten Dienstleistern.
- Cyber-Kriminalität nimmt zu und wird immer ausgefeilter. Der Kunstmarkt / Kunsthandel ist hierbei unter anderem aufgrund der Begehrlichkeit der gespeicherten Kundendaten eine Branche, die zunehmend in den Fokus gerät.
- Selbst bei zunächst vermeintlich geringem Schaden sind die Folgekosten zur Behebung des Datenverlustes nicht zu unterschätzen. Die Kosten eines Cyber-Schadens können häufig nicht ohne weiteres aus der eigenen Liquidität im Unternehmen bestritten werden.
- Die Gesetzgebung und Rechtsprechung zum Datenschutz haben sich signifikant verschärft.
  Wenn Daten Dritter betroffen sind, stellen Cyber-Angriffe regelmäßig auch eine Datenschutzverletzung dar, wenn z. B. eine Veränderung, ein Verlust oder ein unbefugter Zugriff auf personenbezogene Daten erfolgt ist. Diese Vorfälle müssen nach §33 Abs. 1 DSGVO innerhalb von 72 Stunden den zuständigen Datenschutzbehörden gemeldet werden und eine konkrete Beschreibung des Sachverhalts enthalten. Im Falle einer Verletzung der Sicherheitsvorkehrungen zur Speicherung von Daten Dritter können hohe Bußgelder verhängt werden.

Preventum

Art Insurance

Kontaktieren Sie uns

Wir gestalten für Sie ein Versicherungskonzept
passgenau für Ihre Bedürfnisse und Risiken –
zu Ihrem Schutz und dem Ihrer Kunden.

+49 (0)40 325 03 79 – 60
info@preventum-aib.com

Preventum GmbH
Am Sandtorkai 76
D-20457 Hamburg