EIN HACKERANGRIFF KANN JEDEN JEDERZEIT TREFFEN!

Ein falscher Klick in einer E-Mail eines Lieferanten reicht aus und die Soft- und Hardware der eigenen Firma wird infiziert und es kann nicht mehr gearbeitet werden – große finanzielle Schäden für das betroffene Unternehmen sind die Folge. Der Verdienstausfall kann u. U. die Existenz kosten.

Die gute Nachricht – Cybersicherheit ist planbar: Für VHV CYBERPROTECT-Kunden übernehmen wir die Kosten der auswählbaren Präventionsmaßnahmen, die im Rahmen der Cyber-Sicherheitsplattform Cyber-Fuchs angeboten werden. Mitarbeiter werden auf Methoden von Cyberattacken sensibilisiert. Mit diesem firmeneigenen „Frühwarnsystem“ kann das Risiko eines Cyberangriffs erfolgreich abgewehrt werden.

LEISTUNGSINHALTE DER VHV CYBERPRÄVENTION

Damit es gar nicht erst zum Schaden kommt, sollten Firmeninhaber das Präventionsangebot für Mitarbeiter in ihrer Firma integrieren.

- **Awareness-Schulungen** für die Mitarbeiter – in ca. 84 % aller Schadenfälle hat eine Unaufmerksamkeit der Mitarbeiter den Cyberschaden verursacht. Durch Sensibilisierung im Umgang mit digitalen Medien werden Mitarbeiter aufmerksamer, die Risiken eines unbedachten Klicks werden signifikant gesenkt.
- **Richtliniengenerator** – damit Mitarbeiter wissen, wie sie mit digitalen Informationen, Daten und Passwörtern umzugehen haben: allen voran Kundendaten, Zahldaten, personenbezogene Daten bis hin zu besonders schützenswerten Daten.
- **Phishingsimulation** – über 80 % aller erfolgreichen Hackerangriffe beginnen mit einer Mail. Die Mitarbeiter bekommen Mails, mit denen sie dazu verleitet werden sollen, einen Link zu öffnen. Durch unsere Phishingmail-Simulationen lernen die Mitarbeiter, worauf sie achten müssen, um die trickreichen Methoden der Cyberkriminellen zu entlarven. Damit wird mittelbar die IT-Sicherheit des Unternehmens geschützt, weil Firmeninhaber nach jeder Kampagne eine anonymisierte Auswertung erhalten.
- **Darknet-Scan** – Cyberkriminelle tauschen regelmäßig Informationen zu Unternehmen (den potenziellen Opfern) jeglicher Branchen und Firmengrößen im Darknet aus. In der Regel sind das: Mailadressen, Passwörter, Telefonnummern oder auch z. B. Kreditkartendaten. Mithilfe des Darknet-Scans wird das Darknet nach Daten von Kunden der VHV CYBERPROTECT durchsucht. Wir benachrichtigen den Kunden im Ernstfall und schlagen konkret geeignete Schutzmaßnahmen vor.

Die Präventionsangebote von unserem Partnerunternehmen Cyber-Fuchs sind für Kunden von VHV CYBERPROTECT unentgeltlich. Die Kosten werden während der Vertragslaufzeit von der VHV übernommen.

DURCH UNSER PRÄVENTIONS-ANGEBOT SCHÜTZEN SICH FIRMEN VOR EMPFINDLICHEN STRAFEN!

DATENSCHUTZVORFÄLLE BERGEN EIN HOHES FINANZIELLES RISIKO FÜR DEN FIRMENINHABER

Meistens schon vergessen – Datenschutzrichtlinie gemäß DSGVO:
Firmeninhaber übersehen häufig, dass Cyberangriffe in der Regel auch immer einen Datenschutzvorfall beinhalten. Sobald personenbezogene Daten (beispielsweise von Kunden, Geschäftspartnern oder Mitarbeitern) abhandenkommen, muss ein Datenschutzvorfall an die Datenschutzbehörde gemeldet werden. Diese prüft den Sachverhalt und gibt teilweise auch vor, ob und in welcher Form die betroffenen Personen benachrichtigt werden müssen.

Es werden oftmals Bußgelder fällig: Die Höhe des Bußgelds ist abhängig von den Maßnahmen des Geschäftsführers in der Firma!
Bei Datenschutzvorfällen kann die Datenschutzbehörde empfindlich hohe Bußgelder (bis 20 Mio. Euro oder 4 % des weltweiten Umsatzes, je nachdem welcher Wert höher ist) verhängen. Die Höhe des Bußgelds richtet sich auch nach dem Grad des Verschuldens des Unternehmens.

VORTEILE PRÄVENTIONSMASSNAHMEN FÜR FIRMENINHABER

Eine Cyberpolice deckt Risiken ab, die z. B. über Haftpflicht- und Sachversicherungen nicht abgesichert sind. Cyberversicherungen haben daher Vorrang vor allen anderen Policen, wie beispielsweise Haftpflicht- und Sachdeckungen sowie technischen Versicherungen.

- **Minderung des Bußgelds** gegen den Firmeninhaber durch Integration von Präventionsmaßnahmen für Kunden von VHV CYBERPROTECT. Integrierte Präventionsmaßnahmen können **im Schadenfall enthaftend gegenüber Datenschutzbehörden oder Gesellschaftern wirken.**
- **Präventionsmaßnahmen werden laufend für den Firmeninhaber dokumentiert.** Die Dokumentation der Maßnahmen erfolgt automatisch. Sollte es doch zu einem Schadenfall kommen, kann die Geschäftsführung so nachweisen, dass Präventionsthemen im Umgang mit digitalen Medien geschult wurden. Diese Nachweise sind hilfreich bei der Enthaftung gegenüber der Datenschutzbehörde oder den Gesellschaftern eines Unternehmens.

WIE KÖNNEN FIRMENINHABER DAS PRÄVENTIONSANGEBOT NUTZEN?

Ganz einfach: Nach Abschluss der VHV CYBERPROTECT erhalten die Kunden einen Brief mit individuellem Code zur freiwilligen kostenlosen Anmeldung auf der Präventionsplattform. Auf der Plattform werden die Kunden dann komfortabel durch den Anmeldeprozeß geleitet.

Wenn trotz Präventionsmaßnahmen ein Schadenfall entsteht, dann können sich die Kunden auf unsere IT-Experten verlassen.
VHV CYBERPROTECT übernimmt die finanziellen Folgen nach einem Schaden und unterstützt mit ausgewiesenem IT-Know-how, den betroffenen Betrieb so schnell wie möglich wieder arbeitsfähig zu machen. Unsere IT-Forensiker stehen für diesen Fall 24 Stunden an 7 Tagen die Woche das ganze Jahr zur Verfügung! Deutschlandweit sind unsere Experten an über 370 Standorten vertreten.

Besonderheit: Sofern für die Wiederherstellung der Daten und des IT-Systems der eigene IT-Dienstleister beauftragt wird, übernimmt VHV CYBERPROTECT auch hierfür die Kosten.

400.0031.67 Stand 04.2023 Druck 04.2023