BPS – Highlights
CyberPolice

Service-/Kostenbaustein	
Kosten für Forensik/Schadenfeststellung	✓
Benachrichtigungskosten/Call-Center-Leistungen	✓
Kosten für IT-Sicherheitsberater	✓
Rechtsanwaltskosten	✓
Kosten für PR-Berater/Reputation	✓
Aufwendungen vor Eintritt eines Versicherungsfalls	✓
Baustein Eigenschäden (sofern vereinbart)	
Wiederherstellungskosten von Daten/Programmen/Netzwerken	✓
Betrug – Phishing/Pharming	✓
Schäden aus Erpressung/Bedrohung (ohne Lösegeld)	✓
Vertrauensschäden durch eigene Mitarbeiter (ohne Abfluss von Vermögenswerten/Geld)	✓
Betriebsunterbrechung (Haftzeit 120 Tage)	sofern vereinbart (SB 24 Stunden)
Baustein Drittschäden (sofern vereinbart)	
Wiederherstellungskosten von Daten/Programmen/Netzwerken	✓
Ansprüche wegen Vermögensschäden aus Malware/(D)DoS-Attacken	✓
Ansprüche wegen Datenverlust nach Übermittlung von Dateien	✓
Ansprüche aus Verletzung des Datenschutzes	✓
Forderungen der Payment-Card-Industry, inkl. Vertragsstrafe (Kreditkartenschäden)	✓
Ansprüche aus Persönlichkeitsrechts-, Namensrechts-, Urheber- und Markenrechts-verletzungen und daraus resultierende Verstöße gegen das Wettbewerbsrecht	✓
Ansprüche aus Verletzung des geistigen Eigentums	✓
Vertrauensschäden (ohne Unterschlagung von Geld)	✓

✓ Summarisch mitversichert bis zur Höhe der gewählten Versicherungssummen
SB = Selbstbehalt
Es gilt ein allgemeiner Selbstbehalt von 500 Euro je Schadenfall

SIGNAL IDUNA
gut zu wissen

Dieses Faktenblatt ist ein Auszug des Versicherungsschutzes. Die für Sie geltenden Bedingungen ergeben sich aus den im Vorschlag bzw. Versicherungsschein genannten Bedingungen.

5708001 Feb18

Erläuterungen der Leistungen	
Kosten für Forensik/Schadenfeststellung	Übernahme der erforderlichen Kosten zur Ermittlung der Ursache eines Cyber-Angriffes und zur Feststellung des versicherten Schadens. (z. B. IT-Dienstleister, Sachverständigenkosten, Forensiker)
Benachrichtigungskosten/Call-Center-Leistungen	Wenn Kundendaten durch einen Cyber-Angriff abhandenkommen, steht der Betrieb in der gesetzlichen Pflicht, seine Kunden über den Datendiebstahl zu informieren. Die anfallenden Kosten zur Benachrichtigung der Kunden werden übernommen. Muss sogar ein Call-Center zur Beantwortung der großen Anzahl an Kundenfragen beauftragt werden, werden auch diese Kosten übernommen.
Kosten für PR-Berater/Reputation	Durch einen Cyber-Angriff kann ein Betrieb schnell in Negativpresse geraten. Über die CyberPolice werden Kosten für Maßnahmen (z. B. PR-Berater) zur Erhaltung oder Wiederherstellung der öffentlichen Reputation übernommen.
Vertrauensschäden durch eigene Mitarbeiter (ohne Abfluss von Vermögenswerten/Geld)	Eine bewusste Herbeiführung einer Sicherheitsverletzung durch eigene Mitarbeiter.
Forderungen der Payment-Card-Industry, inkl. Vertragsstrafe (Kreditkartenschäden)	Durch einen Cyber-Angriff können Kreditkartendaten von Kunden ausspioniert werden. Wegen Verletzung der vereinbarten Datensicherheitsstandarts machen Kreditkartenunternehmen vertraglich vereinbarte Strafen geltend. Außerdem werden Aufwendungen für Benachrichtigungen der betroffenen Kunden geltend gemacht. Über die CyberPolice werden die Kosten übernommen.
Aufwendungen vor Eintritt eines Versicherungsfalls	Übernahme der Kosten für erforderliche Maßnahmen, zur Abwendung eines unmittelbar bevorstehenden Schadens (z. B. angedrohte Datenveröffentlichung).
Begriffserklärungen	
Phishing	Der Versuch über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten von Internet-Benutzern zu kommen. Beispiel: Erhalt einer E-Mail, in der unter einem Vorwand aufgefordert wird, sich online über einen Link einzuloggen. Beim Klick auf den Link, gelangt man auf eine täuschend echt nachgebaute Seite deines Kreditinstituts. Durch das Einloggen auf der gefälschten Internetseite, erhält der Täter die Zugangsdaten.
Pharming	Betrugsmethode, die durch das Internet verbreitet wird und im Prinzip eine Weiterentwicklung des klassischen Phishings ist. Dabei werden sogenannte DNS-Anfragen von Internetbrowsern so manipuliert, dass der Benutzer unbemerkt auf gefälschte Webseiten umgeleitet wird.
Malware	Malware ist ein Sammelbegriff für Programme, die dazu entwickelt wurden, Benutzern Schaden zuzufügen. Es gibt zahlreiche Unterarten von Malware - zum Beispiel, Viren, Trojaner, Rootkits oder Spyware. Alle Arbeiten anders und haben verschiedene Aufgaben. Ein Ziel haben Sie jedoch gemein: Ihnen zu schaden.
(D)DoS-Attacken	DDoS-Attacken (Distributed Denial-of-Service-Attacken) legen Webserver oder ganze Netzwerke regelrecht lahm. Mehrere Computer greifen dabei gleichzeitig und im Verbund (Botnetze) eine Webseite oder eine ganze Netzinfrastruktur an. Dies kann sehr schnell zum Ausfall der Server führen. Typische DDoS-Angriffe zielen dabei regelmäßig auf die Überlastung des Access-Link, der Ressourcen der Firewall, der Web- und der Datenbankserver.

5708001 Feb18

Dieses Faktenblatt ist ein Auszug des Versicherungsschutzes. Die für Sie geltenden Bedingungen ergeben sich aus den im Vorschlag bzw. Versicherungsschein genannten Bedingungen.