CRIME Protect : Allianz Cyber Schutz und Euler Hermes - VSV
zusammen: unschlagbar gut !

		Allianz	Euler
Versicherungsbedingungen	**Werbeagentur ; Werbeagentur** **Allianz CyberSchutz** **1.000 Euro SB** **Euler Hermes VSV Smart** **ohne SB**	**500.000 €**	**50.000 €**
Ansprüche von Dritten			
Kunden und Dritte			
	Haftpflichtansprüche Dritter aufgrund vorsätzlichen Handelns eigener Vertrauenspersonen (z.B. Diebstahl, Sabotage)		X
	Datenschutzverletzungen aller Art, auch offline. D.h. personenbezogene Daten werden unberechtigt Dritten zugänglich gemacht.	X	
	Gesetzliche Haftpflichtansprüche wegen Vertraulichkeitsverletzungen	X	
	Gesetzliche Haftpflichtansprüche wegen Verletzung gewerblicher Schutzrechte (fremde Patente), durch eine versehentliche Veröffentlichung (z.B. falscher E-Mail Verteiler)	X	
	Gesetzliche Schadenersatzansprüche von Kunden wegen Datenwiederherstellung oder Betriebsunterbrechnung nach einer Netzwerksicherheitsverletzung, sollten Sie unbeabsichtigt Schadsoftware weiterleiten oder Ihr System für ein Weiterleiten missbraucht werden.	X	
	Gesetzliche Schadenersatzansprüche von Kunden wegen einer Betriebsunterbrechung, die durch eine Netzwerksicherheitsverletzung bei Ihnen entsteht, weil Sie dann Ihre vertraglich geschuldete Leistungen (Lieferung/Dienstleistung) nicht erbringen können.	X	
	Ansprüche wegen rechtswidriger digitaler Kommunikation (z.B.nach Accountdiebstahl : Verleumdung, Verbreitung von Falschmeldungen)	X	
Kreditkartenindustrie			
	Verletzung der Sicherheitsstandards der Kartenherausgeber. Schadenersatz und Vertragsstrafen	X	
Eigenschäden			
Vertrauen Sie Ihren Mitarbeitern? Wirklich? ... Immer?	erlittene vorsätzliche Vermögensschädigung durch eigene Vertrauenspersonen		X
	Schäden durch Verrat von eigenen Betriebs- und Geschäftsgeheimnissen durch Vertrauenspersonen sowie Ersatz des dadurch entgehenden Gewinns		X
100% Schutz vor den Gefahren des Internets u. typischen Betrugsmaschen	Betrug durch Dritte mittels Phishing, Pharming, Spyware, Keylogger, Man in the Middle, gefälschte Zahlungsmittel, Schecks, Wechsel, Anweisungen, Bestellungen und Rechnungen. Überweisungen infolge Datenmanipulation.		X
	Zahlung eines Erpressungsgeldes bei angedrohtem Cyberangriff (z.B. angedrohte sog. DDoS-Attacke) bis 100.000 €	X	
	eigene Datenwiederherstellung nach Cyberangriff und Fehlbedienung (Fehlbedienung bis 100.000 €)	X	
	eigene Betriebsunterechung nach Cyberangriff und Fehlbedienung (Fehlbedienung bis 100.000 €)	X	
	Optional: eigene Betriebsunterbrechung infolge eines Cyberangriffs auf die Server Ihres externen Dienstleisters (z.B. Hosting)	X	
Rechtl. Interessenwahrnehmung und Assistanceleistungen			
	Informationskosten der Betroffenen nach Datenschutzpflichtverletzung	X**	
* bis 5 % ** bis 25% der Vers.Summe	Juristische Begleitung eines behördlichen Datenschutzverfahrens	X**	
Umsatz 750.000	Forensische Dienstleistungen	X**	
Kd.-Daten 5.000	Krisenkommunikation Reputationskosten	X**	X*
Personen 15	Schadenermittlungs- u. Rechtsverfolgungskosten		X*
		869 €	**835 €**
		Gesamt :	**1704 €**

Allianz + EULER HERMES Our knowledge serving your success

Diese Aufstellung gibt nur einen Überblick. Verbindlich sind allein die gültigen Versicherungsbedingungen.

Computerkriminalität - die TOP 5 der Betrugsmaschen

Betrug durch Vorspiegelung einer falschen Identität (Fake President Fraud)

Bei dieser Betrugsmasche geben sich die Täter als ein Organ des versicherten Unternehmens - meist ein Vorstandsmitglied - aus und bitten per E-Mail oder Fax einen Mitarbeiter, der im Unternehmen für die Bankgeschäfte verantwortlich ist, eine dringende Überweisung auszuführen.
Dem Mitarbeiter wird dabei vorgespiegelt, dass es sich um eine höchst geheime und vertrauliche Angelegenheit handelt, von der strategische Weichenstellungen im Unternehmen abhängen. Die Betroffenen, die sich einerseits aufgrund des besonderen Vertrauens durch den Vorstand geschmeichelt fühlen, anderseits aufgrund der angeblichen Wichtigkeit der Transaktion erheblich unter Druck stehen, führen diese Überweisungen meist zügig aus.
Fast immer erfolgen die Geldtransfers auf ausländische Konten, vor allem in Asien und Osteuropa. Fliegt der Betrug dann auf, sind die Konten dort meist leergeräumt oder eine Rückholung wird aufgrund des ausländischen Rechtssystems erheblich erschwert.

Häufig werden gezielt Mitarbeiter in ausländischen Niederlassungen des Unternehmens angesprochen. Das erschwert den Mitarbeitern die persönliche Kontaktaufnahme mit den verantwortlichen Organen im Unternehmen, von dener die vermeintlichen Anweisungen kommen.

Betrug durch Umleitung von Zahlungsströmen (Payment Diversion)

In diesen Fällen geben sich die Betrüger als Geschäftspartner oder Lieferanten des versicherten Unternehmens aus und erreichen durch gefälschte Mitteilungen dass die Bezahlung für Waren oder erbrachte Dienstleistungen auf abweichende Konten erfolgt. Die Umsetzung dieser Form des Betruges wird ermöglicht durch eine gefälschte Mitteilung an das versicherte Unternehmen, dass sich die bisher vereinbarten Bankverbindungen geändert haben und der Zahlungsverkehr nun über die neue Bankverbindung abgewickelt werden soll.

Betrug durch Nutzung einer fremden Identität – „Fake Identity Fraud“

Auch bei diesem Betrugsszenario geben sich die Täter als ein bereits existierender Kunde oder als ein Neukunde des versicherten Unternehmens aus und ordern schriftlich Waren. Mit plausiblen Erklärungen wird dann die Lieferung an eine abweichende Lieferadresse verlangt. Da die Identität einer tatsächlich existierenden Firma genutzt wird, schöpfen die Betrugsopfer zunächst keinen Verdacht. Oft fliegt der Betrug erst dann auf, wenn Zahlungsverzug eintritt und di tatsächlich existierende Firma gemahnt wird. Wird dann die Lieferadresse durch die Polizei überprüft, werden die Geschäftsräume verlassen vorgefunden und die Ware ist selbstverständlich längst weiter verschoben worden.

CRIME Protect : Allianz Cyber Schutz und Euler Hermes - VSV zusammen: unschlagbar gut !

Betrug durch gefälschte E-Mails und Webseiten – „Phishing“

Unter Phishing versteht man gemäß Wikipedia Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen.
Häufig sind in diesen E-Mails Anhänge enthalten, die beim Öffnen Keylogger ode andere Schadsoftware auf dem Rechner des Betrugsopfers installieren, die dem Betrüger Zugang zu Dateien und Passwörtern verschaffen können.

Ziel des Betrugs ist es, mit den erhaltenen Daten beispielsweise Kontoplünderun zu begehen und den entsprechenden Personen zu schaden.
Eine neuere Variante des Phishing wird als Spear-Phishing bezeichnet, worunter ein gezielter E-Mail-Angriff auf eine bestimmte Person oder einen ausgewählten Personenkreis zu verstehen ist - anders als bei herkömmlichem Phishing, wo ein große Anzahl an E-Mails an viele Empfänger versendet werden.

Eine weiterentwickelte Form des klassischen Phishings ist das Pharming, welche auf einer Manipulation der DNS-Anfragen von Webbrowsern basiert, um den Benutzer auf gefälschte Webseiten umzuleiten.

Betrug durch Zugriff auf die elektronische Kommunikation zwischen Unternehmen – „Man-in-the-middle“

Ein Man-in-the-Middle-Angriff ist ein Betrugsszenario, das in Rechnernetzen sein Anwendung findet und wobei der Angreifer die Kommunikation zwischen mehreren Unternehmen abhört.
Der Angreifer steht dabei zumeist virtuell zwischen den beiden Kommunikationspartnern, hat mit seinem System vollständige Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmern und kann die Informationen nach Belieben einsehen und sogar manipulieren.

Dieses Risiko liegt außerhalb des eigenen Betriebsgeländes, weshalb ein Unternehmen in der Regel kaum Einfluß darauf nehmen kann.

Denial-of-Service Attacken (DDoS-Attacken)

Über sogenannte Bot-Netzwerke - das sind Mengen an meist unbemerkt infizierten internettauglichen Geräten, welche dadurch ferngesteuert sein können werden bestimmte Internetadressen durch eine "Überschwemmung" mit Anfrage blockiert. Die Folge ist, dass das angegeriffene System den Dienst quittiert und nicht mehr erreichbar ist. So können Internetshops, Datenbanken oder Rechenzentren von Ihren Kunden abgeschnitten werden. Die Folge ist ein Betriebsausfall verbunden mit Einkommensverlust. Nicht unüblich ist auch die Androhung einer solchen DDoS-Attacke, um von den Betroffenen Gelder zu erpressen.