CYBERSCHUTZ-PAKET

FIDES IT Consultants

Wertvolles schützen

Ist Ihre Firewall so sicher wie Fort Knox oder ähnelt sie doch eher der Verteidigung von Troja? Mit anderen Worten: Kann man bei Ihnen ein vermeintlich harmlos aussehendes Objekt platzieren, das sich dann verselbständigt und Schaden anrichtet? Das ist die Wirkungsweise von sogenannten Trojanern, die analog zum hölzernen Pferd der griechischen Mythologie heute bei Angriffen auf IT-Systeme eingesetzt werden.

Informationstechnologie und das Internet mit seinen vielfältigen Angeboten durchdringen Staat, Wirtschaft und Gesellschaft in immer größerem Maße. Relevante Bereiche des privaten und öffentlichen Lebens werden zunehmend digitalisiert. Dadurch steigt die Bedeutung der Verfügbarkeit und Sicherheit der eigenen IT-Systeme sowie des Cyberraums insgesamt. Deutschlands Unternehmen und staatliche Institutionen werden immer häufiger zum Ziel von Cyberkriminalität aller Art. Hinter den Angriffen stehen vielfach international agierende Akteure, die hochprofessionell und effizient vorgehen. Neue Schwachstellen entstehen in immer kürzeren Zyklen und werden umgehend ausgenutzt.

Seit Jahren sehen Unternehmen Handlungsbedarf, um sich gegen derartige Angriffe zu schützen. Viele sind jedoch mit der konkreten Maßnahmengestaltung und Umsetzung überfordert. Wir stehen Ihnen als Partner zur Seite, um Ihnen dabei zu helfen, Ihren unternehmerischen Eigeninteressen genauso gerecht zu werden wie Ihrer Verantwortung im volkswirtschaftlichen Kontext. Eventuelle Lücken zwischen bereits vorhandenen und notwendigen Schutzmaßnahmen werden dabei in effizienter Weise geschlossen. Angriffe werden wirksam abgewehrt und wertvolle interne Ressourcen bleiben sicher verwahrt.

Unternehmerische und gesellschaftliche Verantwortung übernehmen

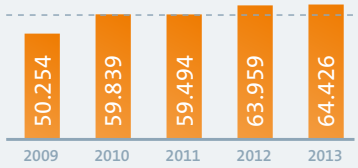
Cyberkriminalität hat in den letzten Jahren stetig zugenommen. Die abgebildete Statistik veranschaulicht diese Entwicklung und zeigt die unterschiedlichen Deliktarten. Unternehmen suchen Schutz und die Bundesregierung trägt dieser Entwicklung mit entsprechenden Gesetzesinitiativen Rechnung. Mit dem modularen FIDES Cyberschutz haben wir ein Produkt zur Abwehr von Angriffen aus dem Internet, wie Cyberspionage oder Datensabotage, und zur Erfüllung gesetzlicher Vorgaben entwickelt.

Das FIDES Cyberschutz-Paket

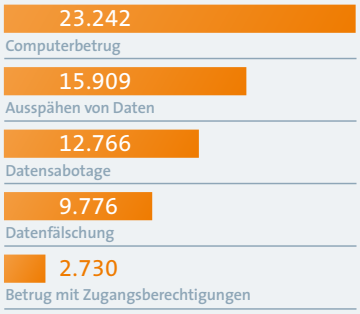
Cyberkriminalität hat in den letzten Jahren stetig zugenommen.

Der größte Anteil der Vorfälle entfällt auf Computerbetrug, die höchsten Zuwachsraten auf Datensabotage.

Cybercrime im engeren Sinne 2009 – 2013



Cybercrime nach Deliktarten 2013



Quelle: Cybercrime Bundeslagebild 2013

Zuerst wird das konkrete, unternehmensindividuelle Schutzniveau definiert, in einem zweiten Schritt mithilfe eines Penetration Tests (d.h. einer Simulation von »Hacking« Angriffen) der IST-Zustand der relevanten IT-Systeme und Komponenten ermittelt und anschließend eventuelle Sicherheitslücken und Schwachstellen durch technische und organisatorische Gegenmaßnahmen geschlossen. Da sich in der IT die Bedrohungslage ständig ändert, bieten wir auf Wunsch eine kontinuierliche Unterstützung zur wirksamen Verteidigung gegen Angriffe an.

Massstäbe setzen - Anforderungsdefinition

Wir helfen Ihnen, die gewährten Freiheitsgrade für die Definition Ihres SOLL-Cyberschutzes in effizienter Weise zu nutzen und gleichzeitig alle einschlägigen Standards zu berücksichtigen. Bekannte Schwachstellen werden angemessen adressiert und sichergestellt, dass diese nicht ausgenutzt werden können. Hohe Ansprüche an die unternehmenseigene IT-Sicherheit und Dienstleistungsverfügbarkeit schaffen Kundenvertrauen und schützen die Reputation Ihres Unternehmens.

Auf Bestehendes aufbauen – IST-Evaluation und Penetration Testing

Auf der Grundlage der für Ihr Unternehmen angelegten SOLL-Anforderungen evaluieren wir vorhandene, risikobehaftete IT-Systeme und -Prozesse. Dazu führen wir u. a. einen Penetration Test durch, bei dem die Sicherheit Ihres Netzwerks über diverse Zugangswege mit den Mitteln eines »Hackers« geprüft wird. Beispielsweise identifizieren wir mit Port- und Security Scannern sowie Exploit-Sammlungen Sicherheitslücken, die u. a. aus nicht eingespielten Sicherheitsupdates resultieren. Auch decken wir fehlende oder ungenügende Passworteinstellungen auf und prüfen die erfolgte Änderung der Standard-Passwörter. Als Ergebnis zeigen wir auf, ob die vorhandenen Schutzmaßnahmen ein Eindringen und Ausnutzen von bekannten Schwachstellen präventiv und angemessen erschweren.

Zielgerichtet vorgehen – Konzeption und Implementierung

Anhand der Analyseergebnisse konzipieren wir mit Ihnen Maßnahmen, um aufgedeckte und relevante Sicherheitslücken zu schließen, unterstützen Sie bei deren Implementierung und schotten Ihre IT so vor Angreifern wirksam ab. Als oberstes Ziel dabei gilt, Ihre IT-Infrastruktur nachhaltig zu schützen, vorhandene Strukturen zu nutzen und nur dort Anpassungen vorzunehmen, wo dies nötig ist.

Nach erfolgter Implementierung verfügen Sie über ein angemessenes Schutzniveau gegen den Verlust von Know-how, Störungen Ihrer Betriebsbereitschaft und Reputationsschäden. Insbesondere für die letzte Schadenskomponente existiert heute am Markt keine wirksame Versicherungsmöglichkeit. Dies räumt der Prävention eines Schadensfalls höchste Priorität ein.

An einem Strang ziehen – Inhouse Schulung

Damit ein einmal erreichtes Sicherheitsniveau erhalten bleibt, informieren und schulen wir Ihre Mitarbeiter zu den einzuhaltenden Sicherheitsvorkehrungen. In Aufbaumodulen für IT-Sicherheitsbeauftragte wird das Wissen zum Cyberschutz weiter vertieft (u.a. zu Meldepflichten gegenüber dem zuständigen Bundesamt vor dem Hintergrund unternehmerischer Diskretion). Schulungsinhalte und -didaktik stimmen wir individuell für Ihr Unternehmen ab.

Wirksamen Schutz erhalten – Kontinuierliche Begleitung

Auf die Wirksamkeit der getroffenen Schutzmaßnahmen müssen Sie und Ihre Mitarbeiter sich verlassen können. Wir unterstützen Sie daher bei der Beobachtung und Anpassung Ihrer Schutzmaßnahmen vor dem Hintergrund relevanter Entwicklungen in der Cyberkriminalität und stehen Ihren IT-Sicherheitsbeauftragten mit Rat und Tat zur Seite.

Als Ergebnis unserer ganzheitlichen und nachhaltigen Konzeption von IT-Schutzmaßnahmen schützen Sie die dauerhafte Leistungsfähigkeit Ihrer IT-Systeme und können sich auf Ihr Kerngeschäft konzentrieren. Ihre Fragen zum Thema Cyberschutz beantworten wir Ihnen gerne im persönlichen Gespräch. Wir freuen uns auf Ihren Anruf.

KONTAKT

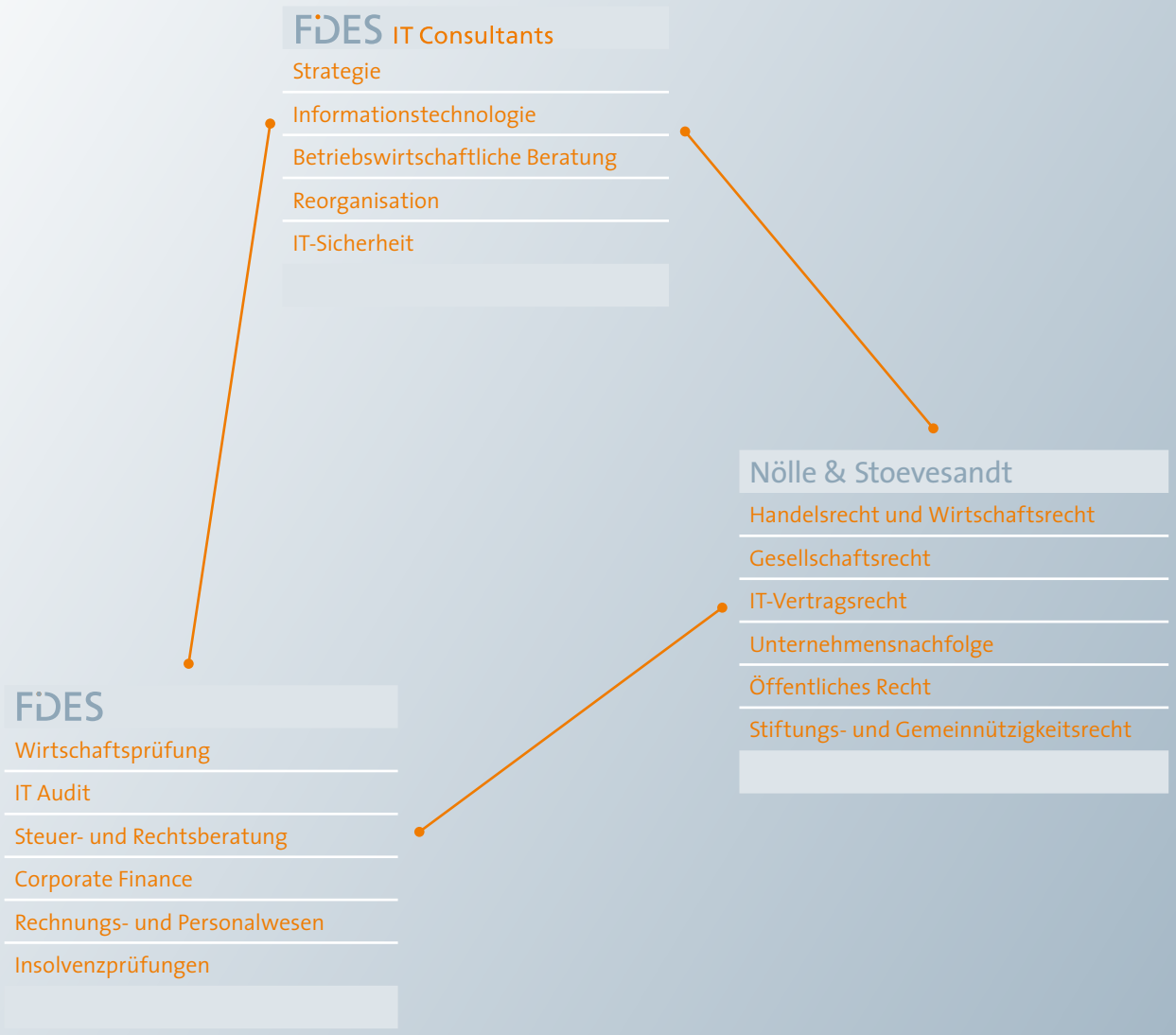
FIDES IT Consultants GmbH
Birkenstraße 37
28195 Bremen
+49 (0)421 3013 400

kontakt@fides-it-consultants.de
www. fides-it-consultants.de

FIDES IT Consultants GmbH
Am Kaiserkai 60
20457 Hamburg
+49 (0)40 23 631 470

kontakt@fides-it-consultants.de
www. fides-it-consultants.de

FEIN ABGESTIMMT – FIDES GRUPPE



Die FIDES IT Consultants sind integraler Bestandteil der FIDES Gruppe. Diese betreut ihre Kunden und Mandanten in interdisziplinären Teams von Spezialisten: Wir sind IT-Consultants, IT-Prüfer, Unternehmensberater, Wirtschaftsprüfer, Steuerberater und Rechtsanwälte. An unseren Standorten haben wir die Kapazitäten vor Ort – an der Schnittstelle zu unseren Kunden und Mandanten. Sie finden bei uns Kompetenz zum Anfassen, Kontinuität in der Begleitung Ihrer Projekte und die Fähigkeit zum Erfolg. Und natürlich Zeit – Zeit für Ihre Probleme, denn gute Beratung fängt immer beim aufmerksamen Zuhören an.