FIDES
Wir sind Vertrauen.

KRITISCHE INFRASTRUKTUREN (KRITIS)

Wir sind Ihr Partner für die Umsetzung der gesetzlichen Vorgaben für Unternehmen der Kritischen Infrastruktur.

IHR ANSPRECHPARTNER

Björn Haje
Manager
b.haje@fides-online.de
Tel.: +49 (421) 3013-415

Betreiber Kritischer Infrastrukturen sind seit 2015 durch das IT-Sicherheitsgesetz verpflichtet, ihre IT-Sicherheit nach dem „Stand der Technik“ umzusetzen. Das ist keine leichte Aufgabe. Denn IT-Sicherheit ist im 21. Jahrhundert ein weites Feld. Es reicht vom abgeschlossenen Serverschrank bis zu organisatorischen Regelungen im Unternehmen. Obwohl KRITIS- Betreiber schon reichlich in die IT-Sicherheit investieren, sind bei den meisten Unternehmen Anpassungen notwendig. Mittelständler haben im täglichen Geschäft oft keine IT-Abteilung, die über ausreichend Kapazitäten verfügt, derartige Change-Prozesse zu stemmen.

Wir unterstützen Sie dabei, die Anforderungen des Gesetzgebers zu erfüllen. Sowohl technisch als auch organisatorisch, von der Aufrechterhaltung des Betriebs bei Hardwareausfällen bis zum Schutz gegen Cyberkriminelle.

Was wir bei kritischen Infrastrukturen für Sie tun:

- KRITIS-Bestandsaufnahme: Wir analysieren, ob Sie Kritische Infrastruktur sind.
- Kontaktstelle zum BSI: Wir begleiten und planen die Einrichtung.
- IT-Sicherheitsmanagement (ISMS): Wir entwerfen gemeinsam mit Ihnen ein ISMS.
- IT-Security: Wir erstellen einen Maßnahmenkatalog und setzen ihn mit Ihnen um.
- IT-Audits: Wir analysieren Ihre IT und identifizieren notwendige Maßnahmen zur Erfüllung der gesetzlichen Anforderungen.
- Technologieberatung: Wir finden skalierbare und exakt auf Ihr Unternehmen abgestimmte IT-Lösungen.

FIDES
Wir sind Vertrauen.

Wenn Sie als Betreiber kritischer Infrastruktur gelten, finden wir gemeinsam mit Ihnen eine sichere und an Ihr Unternehmen angepasste Lösung.

IST IHR UNTERNEHMEN TEIL DER KRITISCHEN INFRASTRUKTUR?

Das IT-Sicherheitsgesetz ist keine Formel, die zweifelsfrei auf jeden Sachverhalt angewandt werden kann. Deswegen ist es keine triviale Frage, ob ein Unternehmen Kritische Infrastruktur ist. Es hängt von mehr als, zum Beispiel, dem reinen Produktionsvolumen ab. Der erste Schritt ist also, gemeinsam mit Ihnen herauszufinden, ob Ihr Unternehmen überhaupt vom BSIG betroffen ist – und ob Sie dann mit dem Bundesamt für Sicherheit in der Informationstechnik in Kontakt treten müssen.

MITTELSTÄNDLER KÖNNEN UNWISSENTLICH DIE KRITIS-GRENZE ÜBERSCHREITEN

Es gibt einige mittelständische Unternehmen in Deutschland, die unwissentlich zur Kritischen Infrastruktur gehören. Oft sind das solide, traditionsreiche Unternehmen, die nicht bewusst verschweigen, dass sie Kritische Infrastruktur sind. Diese Unternehmen fühlen sich vom BSIG gar nicht angesprochen. Das kann ein Lebensmittelhersteller sein, der in den letzten 20 Jahren immer weitergewachsen ist und inzwischen eine halbe Millionen Menschen mit Nahrungsmitteln versorgt, ohne sich darüber wirklich bewusst zu sein. Oder ein Logistiker, der in der Globalisierung expandiert hat. Deswegen sollten alle größeren Mittelständler einmal reflektieren, ob eine Prüfung angebracht ist. Wir ziehen unseren Hut vor der Verantwortung, die KRITIS-Betreiber übernehmen. Die Gesetzeslage ist aber: Wer sich als Betreiber Kritischer Infrastruktur gar nicht beim BSI meldet, muss in Zukunft verstärkt mit Bußgeldern rechnen.

UNSERE LEISTUNGEN FÜR UNTERNEHMEN DER KRITISCHEN INFRASTRUKTUR: EIN WERKZEUGKASTEN, DEN WIR INDIVIDUELL AUF SIE ANPASSEN

Wenn Sie Betreiber Kritischer Infrastruktur sind, müssen wir zunächst gemeinsam erarbeiten, in welchem Bereich Sie Hilfe benötigen. Das kann ganz unterschiedlich sein. Hier sind nur zwei Beispiele für unterschiedliche Schwerpunkte beim Thema Kritische Infrastrukturen

- Wir haben Mandanten mit exzellenten hauseigenen IT-Experten. Diese Unternehmen brauchen eher Hilfe in der Projektierung und Risikoanalyse.
- Dann wiederum gehören Versicherungskonzerne zu unseren Mandanten. Die sind brillant in der Risikoanalyse – da helfen wir eher in den organisatorischen Bereichen, schreiben IT-Strategien und unterstützen das IT-Projektmanagement.

PRAXITY™
Empowering Business Globally

FIDES
Wir sind Vertrauen.

WIR UNTERSTÜTZEN SIE BEI DER IMPLEMENTIERUNG VON IT-SICHERHEITSMASSNAHMEN NACH STAND DER TECHNIK UND NACH VORGABEN DES BSI

IT-Sicherheit nach Stand der Technik bedeutet unter anderem ein dokumentiertes IT-Sicherheitsmanagementsystem. Zwar ist eine einwandfrei gesicherte IT-Infrastruktur generell notwendig, auch unabhängig von Verpflichtungen aus dem BSIG. Für viele Unternehmen bedeutet die Aufrüstung der IT-Sicherheit aber neben Investitionen auch, dass sich ein Stück der Unternehmenskultur und Arbeitsweise verändern muss. Wir finden: Diese Veränderungen sind für viele Unternehmen auch eine Chance, die digitale Transformation sicher anzugehen. Denn IT-Sicherheit ist für Unternehmen überlebenswichtig – auch abseits der Kritischen Infrastruktur.

Die technische Ebene der IT-Sicherheit: Verteidigungsanlagen gegen Cyber-Angriffe

Wir begleiten Sie selbstverständlich auf der technischen Ebene: sichere Netzwerklösungen, Firewalls, Intrusion Detection, Segmentierung. Dafür haben wir im Hause Sicherheitsexperten. Gemeinsam mit Ihnen reorganisieren und optimieren wir Ihre IT-Infrastruktur und unterstützen Sie dabei, Hardware, Software und Netzwerke auszuwählen, die den Vorgaben zur Kritischen Infrastruktur genügen. Dazu zählt auch eine Risikoanalyse Ihrer IT-Infrastruktur und Penetrationstests. IT-Sicherheit bedeutet auch Ausfallsicherheit. IT-Schäden entstehen immer wieder durch Feuer, Hochwasser, Kurzschlüsse oder Fehlbedienung. Hier braucht es professionelle, Redundanzen und Backuplösungen. Wir analysieren gemeinsam mit Ihnen, wie die IT im direkten Betrieb gegen Eindringlinge gesichert ist. Ist der Zugang zum Serverraum gesichert? Ist der Brandschutz im Serverraum gewährleistet?

"Im Unterschied zum Systemhaus sind wir bei IT-Konzepten völlig unabhängig von Herstellern oder Produkten. Wir beraten unter Sicherheitsaspekten und mit Ihren Strukturen im Blick."

Björn Haje, Manager

Wenn jemand die IT eines Unternehmens angreifen möchte, gibt es unzählige Möglichkeiten – aber grob können wir zwei Kategorien unterscheiden:

1. Der Angreifer versucht es über den digitalen Weg und versucht von einem Computer in das Firmennetzwerk einzudringen, Malware oder andere Schadprogramme einzuschleusen oder mit seinen Ressourcen einen DDoS-Angriff durchzuführen.

2. Unsere Analysen zeigen aber auch oft, dass Angreifer ganz einfach auf das Gelände des Unternehmens kommen. Im schlimmsten Falle können Eindringlinge bis an Arbeitsrechner oder gar bis zum Serverraum vordringen. Aber auch der Zugang zu einem Switch auf dem Flur reicht oft, um erheblichen Schaden anzurichten.

FIDES
Wir sind Vertrauen.

Die Anforderungen, die das IT-Sicherheitsgesetz an Betreiber Kritischer Infrastrukturen stellt, sind also multidimensional. Wir helfen methodisch dabei, das Unternehmen sicherer zu machen.

Organisatorische Ebene: Die Koordination der IT-Sicherheit nach innen

Ein wichtiger organisatorischer Schritt ist eine Risikoanalyse nach innen. Und dann müssen wir mit Ihnen Prozesse etablieren, die eine kontinuierliche Weiterentwicklung der IT-Sicherheit gewährleisten.
Auf dieser Ebene führen wir außerdem das IT-Sicherheitsmanagement ein und etabliere die Meldestelle zum BSI. Für das Meldewesen müssen wir Antworten auf folgende Fragen finden:

- Was ist ein meldepflichtiger IT-Vorfall?
- An welcher Stelle fließen die dafür nötigen Informationen zusammen?
- Was sind die konkreten Schritte, wenn ein Sicherheitsvorfall bekannt wird?
- Wer soll Vorfälle an welcher Stelle in der IT bemerken und ist verantwortlich?

Hier müssen wir gemeinsam Prozesse definieren und verankern. Bei der Meldepflicht für IT-Vorfälle gibt es zudem Interpretationsfragestellungen. Wir geben Ihnen gerne Hilfestellungen, wie die Vorgaben des BSI an das Meldewesen zu interpretieren sind.

Wir verstehen, dass Unternehmer eher gehemmt sind, negative Vorfälle zu melden. Die Empfehlung von uns ist aber, auch in Zweifelsfällen an das BSI zu melden – nach aktuellem Stand sind daraus keine Nachteile zu erwarten.

Es ist wichtig, alle Mitarbeiter auf die Reise zu einer sicheren IT mitzunehmen, aufzuzeigen, warum wir etwas verändern müssen. Meistens ist es sinnvoll, diese Veränderungen parallel zur Einführung des Informationssicherheitsmanagementsystems (ISMS) regelmäßig an die Mitarbeiter zu kommunizieren.

WIR UNTERSTÜTZEN IT-ENTSCHEIDER BEI DER KOMMUNIKATION

KRITIS bedeutet fast immer neue Investitionen in die IT-Sicherheit – auch wenn vorher schon ein IT-Sicherheitskonzept bestand. Das ist manchmal gar nicht so einfach an die entscheidenden Stellen zu kommunizieren. Der Grund: Funktioniert alles, ist die IT-Abteilung unauffällig. Funktioniert nicht alles, fällt die IT negativ auf. Das führt viele kleine IT-Abteilungen im Mittelstand zum Dilemma der Messbarkeit von Sicherheit. Ein nicht entstandener Schaden ist wirtschaftlich schwer zu beziffern.

Prävention ist schwer in Geldwerten abzubilden. Das trägt dazu bei, dass die Chefetage die Notwendigkeit größerer Investitionen in moderne Back-up-Lösungen, Intrusion Detection Systeme oder Disaster Recovery nicht sieht. „Es ist ja bisher auch nichts passiert.“ Und wenn dann doch einmal etwas passiert und drei Tage der Wertschöpfung im ganzen Unternehmen verloren sind, ist es zu spät. Wir helfen Ihnen, die Priorität dieser Investition begründet zu kommunizieren und in nachvollziehbare Pakete zu schnüren.

FIDES
Wir sind Vertrauen.

Unsere Aufgabe ist auch, Gesetzestexte für die Entscheider transparent zu machen und Handlungsempfehlungen zu geben.

DIE ANFORDERUNGEN DES BSI BETREFFEN AUCH ABLÄUFE IM BETRIEBSALLTAG

Ausfallsicherheit und Konzepte für die Betriebssicherheit sichern Sie gegen kostspielige Unterbrechungen im Betrieb ab. Mangelhafte IT-Sicherheitsmaßnahmen können im schlimmsten Fall einen wirtschaftlichen oder immateriellen Schaden am Unternehmen zulassen, der es in die Insolvenz bringt. Aber überall, wo Menschen arbeiten, passieren auch Fehler und Unachtsamkeiten.

Die möglichen Quellen für diese menschengemachten IT-Schlupflöcher müssen wir identifizieren und nachhaltig in ein IT-Sicherheitskonzept einbauen.

Gerade Krankenhäuser und Unternehmen mit weitläufigem Betriebsgelände oder viel Besucherverkehr sind anfällig für bewusste oder unbewusste Angriffe auf die IT von innen.

ALLE 2 JAHRE MÜSSEN SIE LAUT BSI PRÜFEN LASSEN, OB DER STAND DER TECHNIK NOCH ERFÜLLT IST

Ob Ihre IT-Sicherheit dem Stand der Technik entspricht muss alle zwei Jahre neu geprüft werden. Unser Audit-Team ist für die Prüfung von Kritischen Infrastrukturen nach § 8a BSIG zertifiziert. FIDES ist als prüfende Stelle beim BSI registriert. Auch das können wir für Sie übernehmen. Dabei prüfen wir Ihre IT-Sicherheit auf die Vorgaben des BSI, identifizieren Deltas und erstellen für Sie einen priorisierten Maßnahmenkatalog.

DAS FAZIT

Benötigen Sie Beratung bei Kritischen Infrastrukturen oder haben eine Frage? Wir stehen gerne persönlich zur Verfügung.