

Schützen Sie sich vor dem Datenklau!



H&D 

International Group

Warum IT-Sicherheit?

Ziel der IT-Sicherheit ist der Schutz von Informationen. Dabei ist Folgendes wichtig:

1. Vertraulichkeit

Informationen müssen vor unbefugter Preisgabe geschützt werden.

2. Verfügbarkeit

Dem Benutzer stehen Dienstleistungen bzw. Informationen zum geforderten Zeitpunkt zur Verfügung.

3. Integrität

Die Informationen sind vollständig und unverändert.

Die in Unternehmen eingesetzte Informations- und Kommunikationstechnologie (ITK) bewirkt eine zunehmende Abhängigkeit der Unternehmen von diesen ITK-Infrastrukturen. Je größer die Gefahr wirtschaftlicher Schäden ist, desto wichtiger ist es, die Verwundbarkeit der eingesetzten Systeme sowie der Netzwerkinfrastruktur zu betrachten und durch geeignete IT-Sicherheitsmaßnahmen zu schützen.



Grundsätzlich ist bei jedem realen (Sicherheits-) System ein Angriff nicht auszuschließen. Es ist daher von besonderer Bedeutung, dass Datensicherung, Katastrophenplanung sowie Maßnahmen für die Wiederherstellung des Regelbetriebes jederzeit funktional und tagesaktuell einsatzbereit sind. So können im Falle eines Vorfalls die Folgeschäden über unmittelbare Verluste hinaus zumindest begrenzt werden.

Einsatz-Szenario

Beispiel Mydoom

Am 27. Januar 2004 nahm die Epidemie eines der bekanntesten Schadenprogramme – des Wurms Mydoom – ihren Anfang.

Mydoom brach den Rekord des Wurms Sobig und löste die bisher größte Epidemie in der Geschichte des Internets aus.

Der Wurm bediente sich der Methode des Social Engineering. Er organisierte einen Angriff auf die Site www.sco.com, die daraufhin ausfiel. Dabei hinterließ er auf den infizierten Computern ein trojanisches Programm, das zur Verbreitung neuer Versionen des Virus benutzt wurde.

Mydoom besaß neben der Funktionalität eines Netzwurms auch eine Hintertür. Verheerend war, dass er neben der Fähigkeit zur Organisation von DoS-Attacken auch über die Funktion eines Keyloggers zum Sammeln von Kreditkartennummern verfügte.



Mögliche Vorgehensweise

Der erste Schritt bei der Beschäftigung mit IT-Sicherheit ist die Bestandsaufnahme:

- Welche Rahmenbedingungen gibt es?
Gesetze, Verträge, Kundenanforderungen, Konkurrenzsituation
- Welche Rolle spielen IT und IT-Sicherheit für das Unternehmen?
- Welche Werte sind zu schützen?
Know-how, Betriebsgeheimnisse, personenbezogene Daten, IT-Systeme
- Was sind mögliche Schadensfälle?

Die „Schutzbedarfstellung“ ist notwendiger Bestandteil jeder Sicherheitsanalyse. Sie soll sicherstellen, dass die definierten Schutzziele und die hieraus abgeleiteten Sicherheitsmaßnahmen angemessen sind und den individuellen Gegebenheiten entsprechen.

Da sich Rahmenbedingungen im Laufe der Zeit ändern können, sollte regelmäßig überprüft werden, ob die ursprüngliche Einstufung noch der aktuellen Situation entspricht. Dabei ist die Orientierung an den drei Grundwerten der IT-Sicherheit: **Vertraulichkeit, Integrität und Verfügbarkeit** hilfreich.

Das tun wir für Sie

„IT-Sicherheit ist kein statischer Zustand, sondern ein dauerhafter Prozess.“

In Anlehnung an den Leitfaden für IT-Sicherheit - BSI

Ein Standard in Deutschland ist der IT-Grundschutz vom BSI (Bundesamt für Sicherheit in der Informationstechnik).

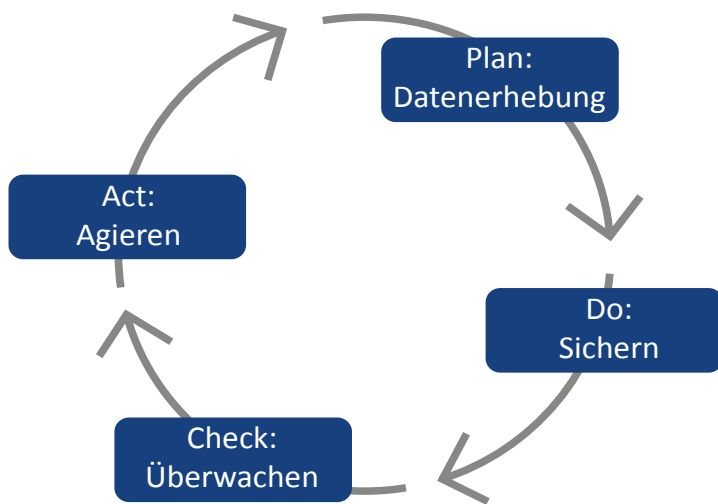
Wir stehen Ihnen als kompetenter Partner zur Seite und führen Audits zur Überprüfung Ihres IT-Sicherheits-Niveaus durch.

Durch ein aktives IT-Sicherheitsmanagement können Schäden verhindert und das Risiken gemindert werden. Gern stehen wir Ihnen beratend zur Seite wenn Sie Unterstützung für Ihren gesamten Sicherheits-Prozess oder in einzelnen Bereichen benötigen.

Mit der Thematik zur Risiko-Analyse und dem Notfallmanagement können wir Ihnen das ganze Spektrum zum IT-Grundschutz anbieten.

So unterstützen wir Sie

Um erfolgreich einen kontinuierlichen Sicherheitsprozess einzuführen, müssen folgende Phasen durchlaufen werden:



Seminare

Die Sensibilisierung der Mitarbeiter für das Thema Sicherheit hat Priorität. Viele Sicherheitsvorfälle entstehen aus Unkenntnis oder mangelnden Problembewusstsein. Wichtig ist die Schulung der Mitarbeiter, damit diese Sicherheitsvorfälle auch als solche identifizieren können und dadurch rechtzeitig die richtigen Maßnahmen ergreifen.

Damit Ihre Mitarbeiter sicherer im Umgang mit den Systemen werden, bieten wir Ihnen ein umfassendes Kursprogramm an. Auf www.letstrainIT.de können Sie unser Schulungsangebot nachlesen. Falls Sie kein passendes Seminar finden sollten, erstellen wir Ihnen gerne ein **individuelles Trainingsangebot**, welches speziell auf Ihre Anforderungen abgestimmt ist.

Planung (Plan)

In der Planungsphase unterstützen wir Sie bei der Einführung von IT-Sicherheit in Ihrem Unternehmen. Dabei werden Richtlinien definiert und darauf aufbauend ein IT-Sicherheitskonzept erstellt. Wir beraten Sie in Fragen der IT-Infrastruktur im Zusammenhang mit der IT-Sicherheit.

Mit unseren verschiedenen Sicherheitschecks zeigen wir Ihnen den aktuellen Stand Ihrer IT-Sicherheit auf.

Außerdem beraten wir Sie bei der:

- Auswahl von IT-Sicherheitsmaßnahmen
- Auswahl einer Methode zur Risikobewertung

Umsetzung (Do)

In dieser Phase werden gezielt die Themen umgesetzt, die in der Planung festgelegt wurden, z. B.:

- Implementierungen aus technischer bzw. organisatorischer Sicht
- Erstellen von aussagekräftigen Dokumentationen
- Einführung neuer Sicherheitsabläufe oder Prozesse
- Realisierungsplan für das IT-Sicherheitskonzept
- Umsetzung von IT-Sicherheitsmaßnahmen
- Schulung und Sensibilisierung

Überwachen / Kontrollieren (Check)

In Ihrem Auftrag führen wir Sicherheits-Audits durch. Dabei wird u. a. der Umsetzungsgrad der beschlossenen Sicherheitsmaßnahmen und die Wirksamkeit, Effizienz und Eignung geprüft.

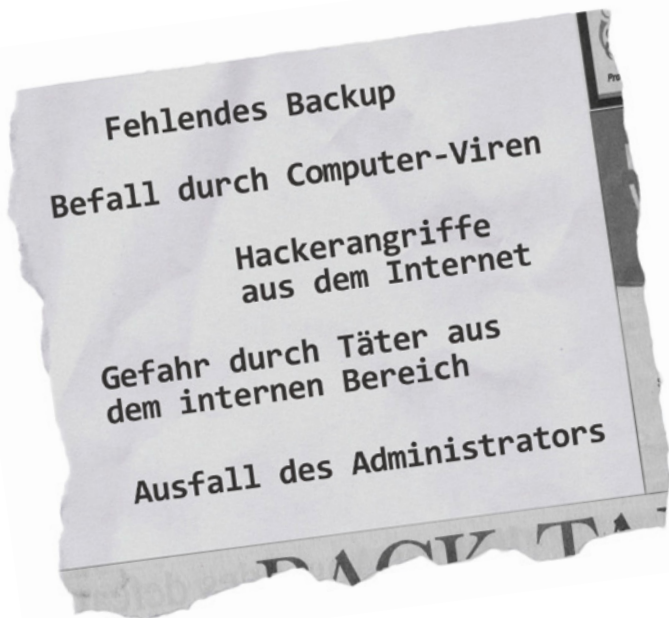
Währenddessen kann festgestellt werden, ob Intervalle für Sicherheitsmaßnahmen verändert werden müssen. Bei einem solchen Audit kann auch das Sicherheitsverständnis Ihrer Mitarbeiter überprüft und ggf. Schulungsmaßnahmen speziell entwickelt werden.

Agieren (Act)

Bei der Verbesserung von IT-Sicherheitsmaßnahmen bzw. bei der Beseitigung von Fehlern stehen wir Ihnen beratend zur Seite.

Sind Ihre sensiblen Daten wirklich sicher genug?

Viel zu häufig passiert es, dass das Unternehmen durch Fehleinschätzungen in solche Situationen geraten kann:



**Schützen Sie sich,
damit Ihnen das nicht passiert!
Wir sagen Ihnen wie!**

Sichern Sie sich die wertvollen Nebeneffekte eines gut durchdachten Sicherheitskonzeptes!

- Sind die Mitarbeiter für IT-Sicherheit sensibilisiert, steigt dadurch die Arbeitsqualität.
- Wartungsarbeiten an IT-Systemen erfordern deutlich weniger Zeit. Administratoren arbeiten effektiver.
- Hieraus ergeben sich für Ihr Unternehmen jede Menge Wettbewerbsvorteile.

Arbeits- und Geschäftsprozesse basieren immer stärker auf IT-Lösungen. Umso wichtiger wird deshalb die Sicherheit und Zuverlässigkeit von Informations- und Kommunikationstechnik.

Mit dem richtigen IT-Sicherheitskonzept wird ein solides Fundament für ein vertrauenswürdiges IT-Sicherheitsniveau gelegt.

Machen Sie jetzt den Sicherheitscheck!

Möchten auch Sie Ihre IT-Sicherheit prüfen?

In Anlehnung an die IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) führen wir einen Sicherheitscheck für Ihre IT durch.

Nach diesem Check erfahren Sie, auf welchem Stand sich Ihr IT-Sicherheitsmanagement befindet und wo eventuelle Sicherheitslücken vorhanden sind.

Sie erhalten über diesen Sicherheitscheck eine ausführliche Dokumentation mit dem Ist-Stand Ihres IT-Sicherheitsmanagements, Vorschläge zur Optimierung und wenn nötig, einer möglichen Umsetzungsstrategie.

Gemeinsam mit Ihnen erarbeiten wir Ihr **Sicherheitskonzept** und beraten Sie in Sicherheitsfragen. Rufen Sie uns unter unserer kostenfreien Rufnummer **0800 4832255** an.



Unsere Standorte



Unternehmensprofil

Die H&D International Group ist ein ganzheitlicher, weltweit tätiger IT-Dienstleister der neuen Generation mit Hauptsitz in Wolfsburg und über 20 Niederlassungen. Seit mehr als 12 Jahren erfolgreich am Markt, beschäftigen wir heute über 1.200 Mitarbeiter in den unterschiedlichsten IT-Projekten. Aufgrund unserer Unternehmensstruktur, unseres vielfältigen Tätigkeitsfeldes und unserer hohen fachlichen Qualifikationen verfügen wir über Problemlösungs-Kompetenzen auf nahezu allen Gebieten der modernen IT. Wir verbinden den Erfahrungs-Background eines internationalen Großkonzerns mit den flachen Hierarchien, der Flexibilität und der Reaktionsgeschwindigkeit eines mittelständischen Unternehmens. Die Hönigsberg & Düvel Datentechnik GmbH ist nach ISO 9001:2008, ISO 20000-1 sowie ISO/IEC 27001 zertifiziert.

H&D Training und Consulting GmbH

Die H&D Training und Consulting GmbH ist als eigenständige Tochter der Hönigsberg & Düvel Datentechnik GmbH tätig. Seit 10 Jahren bieten wir unseren Kunden Seminare, individuelle Workshops, Vor-Ort-Unterstützung sowie Beratung zu folgenden Themen an:

- ✓ IT Service Management
- ✓ Projektmanagement
- ✓ Microsoft Office Anwendungen
- ✓ Netzwerk- und Systemadministration
- ✓ Personal- und Organisationsentwicklung

Microsoft
GOLD CERTIFIED
Partner

Advanced Infrastructure Solutions
Networking Infrastructure Solutions
Information Worker Solutions
Learning Solutions

Kontakt:

H&D Training und Consulting GmbH

August-Horch-Str. 2
38518 Gifhorn

Tel.: 05371 960-0
Fax: 05371 960-210
www.hud-training.de

oder wenden Sie sich an:

Gernot Beu
Consultant
E-Mail: gernot.beu@hud.de