



KNOW**NOW**
TOOLS FOR BUSINESS SUCCESS

Meldung Sicherheitsereignis oder Vorfall

UseNOW - TeachNOW - LearnNOW - FindNOW

- Sofort nutzbar: Auswählen - Anpassen - Anwenden
- In der Praxis erprobt und bewährt
- Im Tagesgeschäft sofort anwendbare Hilfsmittel
- Aktuell durch regelmäßige Updates

Meldung Informationssicherheitseignis oder Informationssicherheitsvorfall

Ihr Vorteil als Know-NOW User:

- **Freie Nutzung kostenloser Tools und Experten-Links**
- **Einrichtung und Nutzung eines Prepay-Kontos**
- **Einsparungen durch attraktive Bonusprogramme**

Informationssicherheitseignis:

Einzelne Ereignisse, die die Informationssicherheit, d. h. die Sicherheit von Verarbeitungen oder den Schutz personenbezogener Daten der Informationssicherheit (Verfügbarkeit, Vertraulichkeit, Unversehrtheit der Daten bzw. Integrität) beeinträchtigen. Ein Ereignis ist ein Vierfachereignis, bei dem die vier Komponenten Sicherheit, Verfügbarkeit, Vertraulichkeit und Integrität der Daten betroffen sind.

Kostenlos und unverbindlich registrieren unter

Sicherheitsvorfall:

www.know-now.de/join

Hinweis:

Bitte füllen Sie die Felder soweit Ihnen die Fakten bereits bekannt sind, sorgfältig aus. Bei Unklarheiten nutzen Sie bitte die Ausfüllhinweise am Ende des Dokuments. Ziehen Sie bei Informationssicherheitsvorfällen die/den Informationssicherheitsbeauftragte(n) hinzu.

Senden Sie diese ausgefüllte Meldeformular per E-Mail an die Adresse:
Ereignis-Vorfall@domain.de.

Sie möchten sich über dieses und weitere **Tools**
informieren?

... nutzen Sie unseren Tool-Online-Shop:
Registrieren und downloaden!

Angaben zur meldenden Person

Ihr Vorteil als Know-NOW User:

- Freie Nutzung kostenloser Tools und Experten-Links
- Einrichtung und Nutzung eines Prepay-Kontos
- Einsparungen durch attraktive Bonusprogramme

Angaben zum Auftreten des Ereignisses bzw. Vorfalls

Zeitpunkt des Vorfalls

Kostenlos und unverbindlich registrieren unter

www.know-now.de/join

Betroffenes System / Datenbank

Angaben zu den Details des Ereignisses bzw. Vorfalls

Detaillierte Beschreibung des Ereignisses / Vorfalls:

Sie möchten sich über dieses und weitere Tools informieren?
... nutzen Sie unseren Tool-Online-Shop:
Registrieren und downloaden!

Angaben zur Einstufung des Ereignisses bzw. Vorfalls

Vertraulichkeit:

Welche Art von Informationen sind
offengelegt

Integrität:

Welche Daten wurden verändert oder manipuliert?

Öffentlich zugängliche Informationen sind betroffen.

Intern geschäftsinnenliegenden wurden kompromittiert.

Vertrauliche Kundeninformationen oder personenbezogene Daten wurden offengelegt.

Offenlegung von für die Information wie geplantes Eigentum oder Sicherheitsdaten wurden kompromittiert.

Es gab keine Beeinträchtigung der Datenintegrität.

Nicht-kritische Daten wurden verändert, aber die Auswirkungen waren gering.

Kritische Geschäftsdaten wurden verändert, was zu Fehlentscheidungen führen könnte.

Manipulierte Daten könnten schwerwiegende rechtliche, finanzielle oder operationelle Folgen haben.

Ihr Vorteil als Know-NOW User:

- Freie Nutzung kostenloser Tools und Experten-Links
- Einrichtung und Nutzung eines Prepay-Kontos
- Einsparungen durch attraktive Bonusprogramme

Kostenlos und unverbindlich registrieren unter

www.know-now.de/join

Verfügbarkeit:

Wie stark ist die Verfügbarkeit von Systemen oder Diensten beeinträchtigt?

Kurzfristige Störung eines unwichtigen Systems, schnell behoben.

Einschränkung der Verfügbarkeit eines wichtigen Systems für mehrere Stunden.

Längerfristige Ausfallzeit eines kritischen Systems, das Geschäft wird erheblich beeinträchtigt.

Komplettausfall von Kernsystemen über längere Zeit, was die Geschäftsfähigkeit massiv beeinträchtigt.

Umfang:

Ein einzelner Arbeitsplatzrechner ist betroffen.

Wie viele Systeme oder Daten sind betroffen?

Mehrere Rechner oder ein Teilnetzwerk sind betroffen.

Ein gesamtes Netzwerksegment oder mehrere kritische Systeme sind betroffen.

Der gesamte Unternehmensbetrieb ist betroffen oder der gesamte Marktstandort.

Sie möchten sich über dieses und weitere Tools

informieren?

Auswirkungen:

Welche direkten und indirekten Auswirkungen hat der Vorfall auf das Unternehmen?

Keine nennenswerten Auswirkungen auf Geschäftsprozesse.

Moderate finanzielle Verluste oder Störungen in Geschäftsfunktionen.

Signifikante finanzielle Verluste, rechtliche Probleme oder langfristige Störungen.

Existenzbedrohende Auswirkungen auf das Unternehmen, einschließlich Marktmacht oder Kundenvertrauen.

... nutzen Sie unseren Tool-Online-Shop:

Registrieren und downloaden!

Angaben zu den durch das Ereignis bzw. den Vorfall betroffenen Daten

Art der (möglicherweise) betroffenen Daten:

Adressen, E-Mail-

Adressen, Kundendaten,

Produktspezifikationen

Dienstleistungskonzepte,

Personendaten, Zeitlinien

Patentdaten, u. ä.

Ihr Vorteil als Know-NOW User:

- **Freie Nutzung kostenloser Tools und Experten-Links**
- **Einrichtung und Nutzung eines Prepay-Kontos**
- **Einsparungen durch attraktive Bonusprogramme**

Kostenlos und unverbindlich registrieren unter

www.know-now.de/join**Angaben zur möglichen Ursache des Ereignisses bzw. Vorfalls**

(Wahrscheinliche) Ursache:

Denial of Service (DoS),
Ausnutzen einer Schwachstelle, Ausnutzen eines Backdoors, u. ä.

Klicken oder tippen Sie hier, um Text einzugeben.

Sie möchten sich über dieses und weitere Tools informieren? ... nutzen Sie unseren Tool-Online-Shop: Registrieren und downloaden!

Ausfüllhinweise bzw. Hilfe zur Nutzung des Formulars

Ihr Vorteil als Know-NOW User:

Angaben zum meldenden User

Name und Rolle: (Rolle = Prozesseigner, Administrator, Sachbearbeiter, usw.)

Telefonnummer, E-Mail: Kontaktdata für den Fall von Rückfragen

- **Freie Nutzung kostenloser Tools und Experten-Links**
- **Einrichtung und Nutzung eines Prepay-Kontos**
- **Einsparungen durch attraktive Bonusprogramme**

Angaben zum Auftreten des Ereignisses bzw. Vorfalls

Bezeichnung / Belebtheit: Aussage darüber, ob es sich um einen Vorfall handelt. Anzeichen eines Hackerangriffs auf den Sharepoint, Diebstahl eines Tablets mit Vertriebsdaten, in der Zeitraum der USB-Stick mit Zugangsdaten

Datum, Uhrzeit des Vorfalls: Sofern bekannt, Angabe wann der Vorfall stattfand.

Datum, Uhrzeit der Kenntnis des Vorfalls: Wann die meldende Person / die betroffene Einheit Kenntnis davon erlangte.

Betroffenes System / Datenbank: Sofern möglich, Angabe welche IT-Infrastruktur, Hard- und/oder Software betroffen ist; ggf. Servername(n).

www.know-now.de/join

Angaben zu den Details des Ereignisses bzw. Vorfalls

Detaillierte Beschreibung des Ereignisses / Vorfalls: Was ist genau passiert?

Möglichst aussagekräftige Beschreibung über die Art des Ereignisses bzw. Vorfalls:

Zum Beispiel: „Bei der Zuordnung von Berechtigungen im Gast-W-Lan, wurde der Zugriff auf interne Laufwerke freigegeben. Dadurch konnten sämtliche Besucher und anwesende Kunden von xx.xx.xxxx bis xx.xx.xxxx auf interne Daten zugreifen.

Angaben zur Einstufung des Ereignisses bzw. Vorfalls

Diese Markierungen dienen der Einstufung, ob es sich bereits um einen Vorfall handelt sowie der Klassifizierung von Sicherheitsvorfällen nach ihrer Schwere. Dies ist die Grundlage, um die richtige Reaktion und Ressourcenallokation sicherzustellen. Bitte immer nur ein Kästchen markieren, da von oben nach unten die Kritikalität zunimmt.

Angaben zu den durch das Ereignis bzw. den Vorfall betroffenen Daten

Art der (möglicherweise) betroffenen Daten: Zum Beispiel Namen, Adressen, Personaldaten, Kundendaten, Produktspezifikationen, Dienstleistungskonzepte, Dokumente (z.B. Kontrakte, Verträge), Gebruichswerten, usw.

Sie möchten sich über dieses und weitere Tools

informieren?

(Wahrscheinlich) Ursache: Was hat zu dem Fehler geführt? Zum Beispiel

menschlicher Fehler durch ungenaues Arbeiten, technisches Problem in der Applikation, Fehlkonfiguration / Sicherheitslücke durch fehlende Updates, die durch einen Hacker ausgenutzt wurde, usw.

... nutzen Sie unseren Tool-Online-Shop:

Angaben zu bereits getroffenen Maßnahmen

Ergriffene Schutzmaßnahmen: Welche Maßnahmen sind ausgeführten

Schutzmaßnahmen, um die Folgen des Vorfalls zu beschränken (z. B. Herunterfahren oder vom Netz nehmen des betroffenen Servers, Sperrung der Benutzer, die von falsch vergebenen Berechtigungen betroffen sind, usw.

Hinweis zur Nutzung des Formulars:

Das Dokument ist abschnittsbezogen als Formular geschützt, sodass Sie z.B. die Kontrollkästen oder Dropdown-Felder (im Sinne eines Formulars) am PC direkt anwählen und ausfüllen können. Es ist kein Kennwort festgelegt.

Schutz entfernen in MS Office 2003:

Symbolleiste „Formular“ aktivieren und auf das „Schloss-Symbol“ klicken.

Schutz entfernen in MS Office 2010:

In der Symbolleiste „Überprüfen“ das Symbol „Bearbeitung einschränken“ aktivieren. Daraufhin öffnet sich das Fenster „Formatierung und Bearbeitung“. In diesem Fenster rechts unten auf die Schaltfläche „Schutz aufheben“ klicken.

Wollen Sie die integrierte Funktionalität nicht nutzen, können Sie die Felder aus der Tabelle einfach entfernen.

Hinweise zur Anpassung des Dokumentes an die Organisation:

Um das Tool an Ihre Dokumentenstruktur anzupassen, gehen Sie (hier am Beispiel der Version MS Office 2010 dargestellt) bitte folgendermaßen vor:

1. Aktivieren Sie in der Leiste „Start“, Gruppe „Absatz“ das Symbol „Alle anzeigen“. Alternativ können Sie in der Leiste „Datei“ auf „Optionen“ klicken, im sich öffnenden Fenster „Anzeige“ auswählen und das Häkchen bei „alle Formatierungszeichen anzeigen“ setzen.
2. Löschen Sie nun zuerst das Textfeld mit dem Titel und danach die Grafik, indem Sie diese Objekte jeweils markieren und die Entfernen-Taste (Entf) betätigen.
3. Danach löschen Sie den verbliebenen Abschnittswechsel (oben), indem Sie diesen markieren und ebenfalls die Entfernen-Taste (Entf) betätigen.
4. Mittels „Doppelklick“ auf die Kopf- oder Fußzeile können Sie diese nun öffnen und die Texte und deren Formatierungen entsprechend Ihren Wünschen gestalten.
5. Löschen Sie das Kopfzeilen-Logo wie vorher, indem Sie dieses markieren und die Entfernen-Taste (Entf) betätigen.
6. Ein neues Logo fügen Sie ein, indem Sie in der Leiste „Einfügen“, Gruppe „Illustrationen“ auf das Icon „Grafik“ klicken und Ihre Datei auswählen.
7. Diese Hinweiseite entfernen Sie, indem Sie (ab dem letzten Seitenumbruch) alles markieren und die Entfernen-Taste (Entf) betätigen.

Nutzungsbedingungen von Fachinformationen:

- (1) Für vorsätzliche oder grob fahrlässige Pflichtverletzungen haftet der Lizenzgeber. Dies gilt auch für Erfüllungsgehilfen.
- (2) Für Garantien haftet der Lizenzgeber unbeschränkt.
- (3) Für leichte Fahrlässigkeit haftet der Lizenzgeber begrenzt auf den vertragstypischen, vorhersehbaren Schaden.
- (4) Der Lizenzgeber haftet nicht für Schäden, mit deren Entstehen im Rahmen des Lizenzvertrags nicht gerechnet werden musste.
- (5) Für Datenverlust haftet der Lizenzgeber nur, soweit dieser auch bei der Sorgfaltspflicht entsprechender Datensicherung entstanden wäre.
- (6) Eine Haftung für entgangenen Gewinn, für Schäden aus Ansprüchen Dritter gegen den Lizenznehmer sowie für sonstige Folgeschäden ist ausgeschlossen.
- (7) Der Lizenzgeber haftet nicht für den wirtschaftlichen Erfolg des Einsatzes der Tools oder Trainings.
- (8) Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt.