



**knownow**  
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 Informationssicherheitsereignis 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

Kostenlos und unverbindlich registrieren unter

[www.know-now.de/join](http://www.know-now.de/join)

Mit diesem Formular müssen Ereignisse oder Vorfälle, die die Informationssicherheit, d. h. die Sicherheit von Verarbeitungen oder den Schutz personenbezogener Daten der Informationssicherheit (Verfügbarkeit, Vertraulichkeit, Unversehrtheit der Daten bzw. System- und Zugänglichkeit) betreffen, gemeldet werden.

**Informationssicherheitsereignis:**

Ein Ereignis, bei dem es eine ausspäthende Reaktion auf einen Sicherheitsvorfall kommen könnte. Ereignisse machen uns darauf aufmerksam, dass Sicherheitsrisiken in der Organisation bestehen.

**Sicherheitsvorfall:**

Einzelnes ungewolltes oder unerwartetes Informationssicherheitsereignis oder eine Reihe von Ereignissen, die eine erhebliche Wahrscheinlichkeit besitzen, Geschäftstätigkeiten zu gefährden und die Informationssicherheit zu bedrohen.

**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

Vor- und Nachname	Klicken oder tippen Sie hier, um Text einzugeben.	Rolle, Funktion	Klicken oder tippen Sie hier, um Text einzugeben.
Telefonnummer	Klicken oder tippen Sie hier, um Text einzugeben.	E-Mail	Klicken oder tippen Sie hier, um Text einzugeben.

## 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

Ort, Datum, Uhrzeit des Vorfalles (soweit bekannt)	Klicken oder tippen Sie hier, um Text einzugeben.
--	---

Kostenlos und unverbindlich registrieren unter

[www.know-now.de/join](http://www.know-now.de/join)

Datum, Uhrzeit des Vorfalles (soweit bekannt)	Klicken oder tippen Sie hier, um Text einzugeben.
Ort, Datum, Uhrzeit des Vorfalles (soweit bekannt)	Klicken oder tippen Sie hier, um Text einzugeben.

Betroffenes System / Datenbank

Klicken oder tippen Sie hier, um Text einzugeben.

## Angaben zu den Details des Ereignisses bzw. Vorfalls

Detaillierte Beschreibung des Ereignisses / Vorfalls:	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!

## Angaben zur Einstufung des Ereignisses bzw. Vorfalls

**Vertraulichkeit:**

Welche Art von Informationen sind in welcher Weise offengelegt worden?

- ☐ Öffentlich zugängliche Informationen sind betroffen.  
Interne Geschäftsinformationen wurden kompromittiert.  
☐ Vertrauliche Kundeninformationen oder personenbezogene Daten wurden offengelegt.  
☐ Geschäftsinterne vertrauliche Informationen wie Geschäftsverträge, Eigentum oder Sicherheitsdaten wurden kompromittiert.

**Integrität:**

Welche Daten sind verändert oder manipuliert?

- ☐ Es gab keine Beeinträchtigung der Datenintegrität.  
☐ Nicht-kritische Daten wurden verändert, aber die Auswirkungen sind geringfügig.  
☐ Kritische Geschäftsdaten wurden verändert, was zu Fehlentscheidungen führen könnte.  
☐ Kritische Daten könnten schwerwiegende rechtliche, finanzielle oder operationelle Folgen haben.

**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:**

Wie viele Systeme oder Daten sind betroffen?

- ☐ Ein einzelner Arbeitsplatzrechner ist betroffen.  
☐ Mehrere Rechner oder ein Teilnetzwerk sind betroffen.  
☐ Ein gesamtes Netzwerksegment oder mehrere kritische Systeme sind betroffen.  
☐ Der gesamte Unternehmensbereich ist betroffen oder der gesamte Betrieb ist betroffen.

**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, technische Probleme oder langfristige Störungen.  
☐ Existenzbedrohende Auswirkungen auf das Unternehmen, massiver Verlust von Marktanteilen oder Kundenvertrauen.

## 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](http://www.know-now.de/join)

Sie möchten sich über dieses und weitere Tools informieren?

... 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, Produkt- und Leistungsdaten, Dienstleistungskonzepte, Personalakten, Zeugnisse, Patentdaten, u. ä.

Klicken oder tippen Sie hier, um Text einzugeben.

## 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](http://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.

## Angaben zu bereits getroffenen Maßnahmen

Eingeleitete

Sofortmaßnahmen:

Informierte Person, Netzverbindung getrennt, System heruntergefahren, Fernlokalisierung, 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 zu meldender Person

**Name und Rolle:** (Rolle = Prozesseigner, Administrator, Sachbearbeiter, usw.)**Telefonnummer, E-Mail:** Kontaktdaten für den Fall von Rückfragen

- Freie Nutzung kostenloser Tools und Experten-Links

Angaben zum Auftreten des Ereignisses bzw. Vorfalls

- Einrichtung und Nutzung eines Prepay-Kontos
- Einsparungen durch attraktive Bonusprogramme

**Bezeichnung / Bezeichnung:** Aussagekräftige Bezeichnung des Vorfalls (Anzeichen eines Hackerangriffs auf den Sharepoint, Diebstahl eines Tablets mit Vertriebsdaten, in Zusammenhang mit einem Sicherheitsvorfall)

**Datum, Uhrzeit des Vorfalls:** Sofern bekannt, Angabe wann der Vorfall stattfand.**Datum, Uhrzeit der Kenntnis des Vorfalls:** Wann die meldende Person / die Organisation Kenntnis vom Vorfall erlangte**Betroffenes System / Datenbank:** Sofern möglich, Angabe welche IT-Infrastruktur, Hard- und/oder Software betroffen ist; ggf. Servername(n).

Kostenlos und unverbindlich registrieren unter

[www.know-now.de/join](http://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, Geschäftsdaten, (Geheim-)Daten, usw.

**Angaben zum möglichen Ursprung des Ereignisses bzw. Vorfalls**

**(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 werden.

**Angaben zu bereits getroffenen Maßnahmen**

**Ergriffene Sofortmaßnahmen:** Sofortmaßnahmen, die umgehend ausgeführt wurden, 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.).

Sie möchten sich über dieses und weitere Tools

informieren?

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

Registrieren und downloaden!

**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 Hinweisseite 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.