RFC 2350 Beschreibung

Cyber-Emergency-Response-Team der EnBW

EnBW-CERT

Inhaltsverzeichnis

1 Dokumentinformationen

In diesem Dokument wird das EnBW-CERT nach RFC 2350 Standard (https://tools.ietf.org/html/rfc2350) beschrieben. Es liefert eine Übersicht über das EnBW-CERT, seine Erreichbarkeit und Aufgaben und Zuständigkeiten sowie diee angebotenen Leistungen.

1.1 Datum der Freigabe und Dokumentenhistorie

Diese initiale Version dieses Dokumentes wurde am 2022-08-01 durch den Informationssicherheitsmanager der FE IT für das frühere EnBW-IT-CERT freigegeben und veröffentlicht.

Version	Gültig ab	Autor	Änderungen
1.0	2022-08-01	Ulrich Stadie	Initiale Version
1.1	2022-09-13	Ulrich Stadie	Anpassung Links
1.2	2023-01-01	Ulrich Stadie	Anpassung/Aktualisierung wegen der Zusammenlegung der beiden CERTs: EnBW-IT-CERT und EnBW-CERT. EnBW-CERT ist der neue Name.
1.3	2023-10-02	Ulrich Stadie	Aktualisierung PGP-Key und S/MIME-Zertifikat
1.4	2024-01-01	Ulrich Stadie	Aktualisierung Liste der Teammitglieder
1.5	2024-09-10	Ulrich Stadie	Entfernen der Teammitgliederauflistung; Layout-Anpassungen; TF-CSIRT/TI Listung des EnBW-CERT hinzugefügt
1.6	2024-12-05	Ulrich Stadie	Aktualisierung S/MIME-Zertifikat

1.2 Verteilerliste für Benachrichtigungen

Keine.

1.3 Verfügbarkeit für dieses Dokument

Die aktuelle Version dieses Dokuments finden Sie auf dem offiziellen EnBW-CERT-Webauftritt:

https://www.enbw.com/cert

Bitte stellen Sie sicher, dass Sie die neueste Version haben.

1.4 Authentizität dieses Dokumentes

Dieses Dokument wurde mittels S/Mime vom EnBW-CERT signiert. Der Fingerabdruck des Schlüssels befindet sich auf dem EnBW-CERT-Webauftritt (siehe Abschnitt 1.3) sowie in diesem Dokument (siehe Abschnitt 2.8.1).

EnBW CERT

EnBW-CERT
2024.12.05
11:59:26
+01'00'

2 Kontaktinformationen

2.1 Namen

EnBW-CERT: Cyber Emergency Response Team der EnBW

2.2 Postanschrift

Energie Baden-Württemberg AG (EnBW)
FE IT
EnBW-CERT
Durlacher Allee 93
76131 Karlsruhe
Deutschland

2.3 Etablierungsdatum EnBW-CERT

Das EnBW-CERT wurde am 1. Januar 2023 offiziell etabliert.

2.4 Zeitzone

CET/CEST,
Mitteleuropäische Zeit/Mitteleuropäische Sommerzeit,
UTC+0100/UTC+0200

2.5 Telefonnummer

Über die EnBW-CERT-Telefonnummer +49 721 63 12130 können dringende Meldungen zu IT-Sicherheitsvorfällen an das EnBW-CERT gemeldet werden.

EnBW-Angehörige können das EnBW-CERT mittels der EnBW-intern bekannten Telefonnummer bzw. über den IT-Support bzw. außerhalb der Dienstzeiten über das ServiceCockpit erreichen.

Mit etablierten Kommunikationspartnern sind auch Telefonkontaktmöglichkeiten ausgetauscht, über die das EnBW-CERT direkt erreicht werden kann.

2.6 Weitere Telekommunikationsmöglichkeiten

Keine.

2.7 E-Mail

Die E-Mailadresse des EnBW-CERT lautet cert@enbw.com.

Für Meldungen von extern an das EnBW-CERT dient primär E-Mail als Eingangskanal, sofern noch kein Austausch von Telefonkontaktdaten stattgefunden hat.
In dringenden Fällen kann [wichtig] in die Betreffzeile aufgenommen werden, um die Dringlichkeit einer Mail anzuzeigen. Für eine verschlüsselte Kommunikation stellt das EnBW-CERT seinen PGP-Schlüssel sowie sein S/Mime-Zertifikat bereit (siehe Abschnitt 2.8).

2.8 Öffentliche Schlüssel und andere Verschlüsselungsinformationen

2.8.1 S/Mime-Zertifikat

Der öffentliche Schlüssel des EnBW-CERT S/Mime-Zertifikats hat den folgenden Fingerabdruck:
11ED 9702 7E43 C5CC D142 2BC1 9C54 B1DF EF77 8B4E

Der öffentliche Schlüssel ist auf der Webseite des EnBW-CERT verfügbar:
https://www.enbw.com/cert

2.8.2 PGP-Schlüssel

Der EnBW-CERT PGP-Schlüssel hat die folgenden Identifikationsdaten:
KeyID: **0xC5060B5003FAAE32**
Fingerabdruck: **C181 39D7 3410 A204 4800 270E C506 0B50 03FA AE32**

Der PGP-Schlüssel ist auf der Webseite des EnBW-CERT verfügbar:
https://www.enbw.com/cert

Zusätzlich ist der PGP-Schlüssel auch auf den üblichen öffentlichen Schlüsselservern veröffentlicht und kann von dort heruntergeladen werden:

- OpenPGP-Public-Key-Server (http://pgpkeys.mit.edu)
- PGP-Global-Directory (https://keyserver.pgp.com)

EnBW-CERT versucht, so viele Unterschriften von anderen Teams oder Einzelpersonen für den öffentlichen EnBW-CERT-Schlüssel zu sammeln, um das PGP-"Web of Trust" zu stärken.

2.9 Angehörige von EnBW-CERT

Das EnBW-CERT veröffentlicht keine Informationen zu den Mitgliedern des EnBW-CERT.

2.10 Betriebsstunden

Die regulären Geschäftszeiten des EnBW-CERT sind Montag bis Freitag von 09:00-17:00 Uhr (außer an Feiertagen).
Darüber hinaus wird vom EnBW-CERT ganzjährig eine 24/7 Bereitschaft für die EnBW gegangen, die über die Alarmierungswege der EnBW erreicht werden kann.

2.11 Weitere Informationen

Allgemeine Informationen zum EnBW-CERT sind auf dem Webauftritt des EnBW-CERT verfügbar:
https://www.enbw.com/cert/

Das EnBW-CERT ist Mitglied in den folgenden Organisationen:

- CERT-Verbund
  http://www.cert-verbund.de

Das EnBW-CERT ist beim TF-CSIRT/TI als Team registriert und strebt eine Akkreditierung als Team an.

- TF-CSIRT Trusted Introducer (TI)
  http://www.trusted-introducer.org/directory/teams/cert-bund.html

Zusätzlich strebt das EnBW-CERT auch die Mitgliedschaft in folgenden Organisationen an:

- FIRST (Forum for Incident Response and Security Teams)
  http://www.first.org/members/teams/cert-bund

2.12 Kontaktmöglichkeiten

Das EnBW-CERT überwacht seine Kontakt-E-Mail-Adresse cert@enbw.com.
Zusätzlich überwacht das EnBW-CERT auch die offizielle Abuse-E-Mailkontaktadresse abuse@enbw.com.
Für das Melden von Sicherheitslücken/Schwachstellen in Software oder auf Webseiten der EnBW ist eine koordinierter Veröffentlichungsprozess eingerichtet. Die Informationen zu diesem sind auf dem Webauftritt des EnBW-CERT verfügbar. Die dafür eingerichtete E-Mailadresse cvd@enbw.com wird ebenfalls vom EnBW-CERT überwacht.

In dringenden Fällen kann [wichtig] in die Betreffzeile aufgenommen werden, um die Dringlichkeit einer Mail anzuzeigen. Für eine verschlüsselte Kommunikation stellt das EnBW-CERT seinen PGP-Schlüssel und S/Mime-Zertifikat bereit (siehe Abschnitt 2.8).

Ebenso kann in kritischen Fällen mittels der Bereitschaftshotline rund um die Uhr ein Kontakt hergestellt werden.
Darüber hinaus werden alle als Sicherheitsvorfall deklarierten Tickets des Ticketing-Systems der EnBW IT dem EnBW-CERT zur Kenntnis gebracht und von dem Bereitschaftsdiensthabenden des EnBW-CERT wahrgenommen.

3 Satzung

3.1 Leitbild

Das EnBW-CERT, als Teil des Informationssicherheitsprozesses der EnBW, fungiert als Anlaufstelle für IT-Sicherheitsvorfälle bei der IT-Leistungserbringung und -Prozessen. Darüber hinaus bietet es bestimmte Dienstleistungen für kritische Infrastrukturen an.

Die Ziele des EnBW-CERT sind
- die EnBW bei auftretenden computersicherheitsrelevanten Vorfällen im Rahmen von reaktiven Maßnahmen zu unterstützen sowie
- die Prozesse/Angehörigen der EnBW bei der Umsetzung proaktiver Maßnahmen zur Verringerung des Risikos solcher Unfälle zu unterstützen.

3.2 Verantwortungsbereich

Der Verantwortungsbereich („Constituency“) des EnBW-CERT ist der gesamte EnBW-Konzern, wie im Kontext der folgenden Richtlinien beschrieben:
- "EnBW-Konzernrichtlinie zur Informationssicherheit"
- "Informationssicherheitsleitlinie der FE IT"

Diese beiden Richtlinien werden im Weiteren in ihrer Gesamtheit als "EnBW-Informationssicherheits-Richtlinien" bezeichnet.

Das EnBW-CERT ist für das folgende autonome System zuständig:
- AS15698

3.3 Sponsoring Organisation / Zugehörigkeit

Das EnBW-CERT ist als das Informationssicherheitsteam für die EnBW benannt. Organisatorisch ist das EnBW-CERT in der Funktionaleinheit IT (FE IT) etabliert und wird darüber auch finanziert.

3.4 Beauftragung und Berechtigungen

Das EnBW-CERT bearbeitet im Auftrag und mit Befugnissen, die dem EnBW-CERT zur Wahrnehmung seiner Aufgaben, insbesondere zur Gefahrenabwehr, vom Leiter der Funktionaleinheit IT (C-TI) und dem CIO der EnBW delegiert wurden. Weitere Informationen zum Mandat und zur Autorität des CIO finden sich in der "EnBW-Informationssicherheitspolitik".

Das EnBW-CERT ist bestrebt mit Systemadministratoren und Anwendern zur Erreichung der Sicherheitsziele der EnBW bestmöglich zusammenzuarbeiten, macht bei Bedarf aber auch von einer Weisungsbefugnis gebrauch.

Mitarbeiter und verbundene Partner der EnBW-Community, die gegen die Aktionen des EnBW-CERT Beschwerde einlegen möchten, sollten sich an den Leiter "IT-Strategie und Digitalisierung" wenden. Wenn die dadurch erreichte Klärung nicht zufriedenstellend ist, kann dies dem CIO der EnBW zur Kenntnis und eventuellen weiteren Würdigung vorgebracht werden.

3.5 Netzwerkbereiche im Verantwortungsbereich

Im Verantwortungsbereich des EnBW-CERT liegen die folgenden öffentlichen IPv4-Netzwerke:

- Autonome System AS15698: 195.35.72.0/21

Im Verantwortungsbereich des EnBW-CERT liegen die folgenden öffentlichen IPv6-Netzwerke:

- 2a0b:cfc0:6000::/44
- 2a0b:f400::/32
- 2a0d:5840::/44
- 2a0d:5840:80::/44
- 2a0d:5840:c080::/41
- 2a0d:5840:ff80::/41

Darüber hinaus ist das EnBW-CERT auch auf verschiedenen cloud-basierten Netzwerken der EnBW verschiedener Cloud-Service-Anbieter (z. B. AWS, Azure, Google) tätig, wenn diese durch die EnBW genutzt werden.
Ebenfalls gehören die verschiedenen privaten Netze, die von C-TI für die EnBW betrieben werden, zum Verantwortungsbereich des EnBW-CERT.

4 Richtlinien und Regelungen

4.1 Klassifizierung von eingehenden Informationen

Alle eingehenden Informationen werden als vertraulich oder höher eingestuft und behandelt. Dieses strenge Klassifizierungssystem verhindert die unbeabsichtigte Offenlegung von Informationen, die durch andere (externe) Klassifikationssysteme klassifiziert werden, die möglicherweise nicht denen von EnBW-CERT entsprechen.

Das EnBW-CERT befolgt bezüglich der Weitergabe vertraulicher Informationen das von der FIRST entwickelte Traffic-Light-Protocol (TLP; https://www.first.org/tlp/). Informationen, die das EnBW-CERT erhält und die gemäß TLP eingestuft sind, werden entsprechend der Einstufung vertraulich behandelt.

Elektronische Informationen werden in der Regel nur auf verschlüsselten Speichermedien gespeichert. Die Schlüsselverwaltung dieser Aufgaben erfolgt nur durch EnBW-CERT-Angehörige.

4.2 Aufbewahrung von Datensätzen

Die vom EnBW-CERT eingesetzten Systeme und Datenträger (persönliche Rechner, Forensiksysteme, Archiv- und Übergabe-Datenträger) sind generell immer grundverschlüsselt.
Die Datensätze, die Informationen zu Sicherheitsvorfällen enthalten, werden mindestens für die Dauer der laufenden Untersuchung und eventueller Gerichtsverwertung verschlüsselt vorgehalten. Dies gilt für Aufzeichnungen, die entweder elektronisch oder als Hardcopy gespeichert werden. Die Löschung dieser Datensätze erfolgt erst, wenn die Vorfallsbehandlung abgeschlossen wurde und es keine weiteren Anforderungen zur Aufbewahrung (z.B. laufende Gerichtsverfahren oder Aufbewahrungsfristen) mehr existieren.
Elektronische Informationen werden in einer zentralen Datenbank des Ticketing Systems "baseIT" der EnBW IT gespeichert. Auf diese Datenbank kann nur über authentifizierte und gesicherte Verbindungen zugegriffen werden. Verschlüsselte Sicherungen dieser Datenbank werden täglich erstellt und in den von der EnBW IT bereitgestellten Backup-Systemen gespeichert.
Papierhafte Aufzeichnungen des EnBW-CERT (z.B. Übergabeprotokolle, Abschlussberichte) werden in den zutrittsgesicherten Räumlichkeiten des EnBW-CERT in verschließbaren Schränken aufbewahrt, die nur für EnBW-CERT-Mitarbeiter zugänglich sind.
Klassifizierte Berichte können für berechtigte Personen zusammengestellt und gedruckt werden. Von sensitiven Informationen bereinigte und nicht klassifizierte Berichte können zu Schulungszwecken erstellt und veröffentlicht werden.

4.3 Löschung und Entsorgung von Datenträgern und Aufzeichnungen

Medien wie Festplatten, Disketten oder Flash-Laufwerke werden nach den Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI) im Rahmen der Entsorgung durch das EnBW-CERT gelöscht, bevor diese zur physikalischen Entsorgung übergeben werden. Alle Löschaktionen von Medien, die zum EnBW-CERT gehören, werden in einer Logdatei aufgezeichnet und nur von EnBW-CERT-Mitarbeitern ausgeführt.
Das Löschen/Vernichten optischer Medien erfolgt durch physische Zerstörung, entweder manuell oder mit einer speziellen Zerkleinerungsmaschine.
Zum Löschen von papierhaften Aufzeichnungen werden diese entweder manuell zerstört oder an einen nach DIN 66399 zertifizierten Dienstleister mittels spezieller Behälter zur Entsorgung übergeben. Ebenso werden auch die Datenträger (nachdem sie durch EnBW-CERT gelöscht wurden) zur Entsorgung konform zur DIN 66399 (ISO/IEC 21964) an den Dienstleister übergeben.

4.4 Arten von Vorfällen und Support-Stufen

EnBW-CERT ist berechtigt, alle Arten von IT-Sicherheitsvorfällen zu adressieren, die innerhalb und gegen den Verantwortungsbereich des EnBW-CERT auftreten.
Der Grad der Unterstützung der Betroffenen durch EnBW-CERT variiert je nach Art und Schwere des Vorfalls oder Problems, dem betroffenen Bereich, die Größe der betroffenen Benutzergemeinschaft und die EnBW-CERT-Ressourcen, die zu diesem Zeitpunkt verfügbar sind, obwohl in allen Fällen eine Antwort gegeben wird. Ressourcen werden, gegebenenfalls nach einer Triage durch EnBW-CERT, nach den folgenden Prioritäten zugewiesen, die in abnehmender Reihenfolge aufgeführt sind:

1. Bedrohungen der physischen Sicherheit von Menschen.
2. Angriffe auf Root- oder Systemebene auf jedes zentrale IT-Management-System oder einen Teil der Backbone-Netzwerkinfrastruktur (onprem und Cloud).
3. Angriffe auf Root- oder Systemebene auf relevante öffentlich erreichbare Systeme (für Multi-User oder dedizierte Zwecke) (onprem und Cloud).
4. Gefährdung eingeschränkter vertraulicher Dienstkonten oder Softwareinstallationen (onprem und Cloud).
5. Denial-of-Service-Angriffe auf eines der oben genannten Systeme (onprem und Cloud).
6. Großangelegte Angriffe jeglicher Art, z. B. Aufklärungsangriffe („sniffing/recon attacks"), "Social Engineering"-Angriffe oder Angriffe auf Passwörter/Loginschnittstellen (onprem und Cloud).
7. Bedrohungen, Belästigungen oder andere Straftaten, die einzelne Benutzerkonten betreffen.
8. Gefährdung einzelner Benutzerkonten auf Mehrbenutzersystemen.
9. Kompromittierung von persönlichen Rechnersystemen.
10. Fälschungen, falsche Darstellungen oder andere sicherheitsrelevante Verstöße gegen lokale Regeln und Vorschriften, z. B. E-Mail-Manipulationen oder unbefugte Nutzung von IRC-Bots.
11. Denial-of-Service-Angriffe auf einzelne Benutzerkonten, z. B. Mail-Bombardements.

Andere als die oben genannten Vorfälle werden entsprechend ihres Schweregrades, Auswirkung und Verbreitung priorisiert.
Endbenutzer werden nicht unmittelbar unterstützt. Von ihnen wird erwartet, dass sie sich an ihre jeweiligen Systemadministratoren, Netzwerkadministratoren, Information Security Manager (ISM) oder Abteilungsleiter zur Unterstützung wenden. Das EnBW-CERT wird die beiden letztgenannten Personengruppen unterstützen.
Das EnBW-CERT versucht der unterschiedlichen Expertise der beteiligten Personen durch Zielgruppen spezifische Information und Unterstützung gerecht zu werden. Im Rahmen der Vorfallsbearbeitung kann keine Schulung oder Systemwartung durch das EnBW-CERT erfolgen. In den meisten Fällen wird das EnBW-CERT Hinweise und Informationen geben, die für die Umsetzung geeigneter Maßnahmen erforderlich sind und ggf. können nützliche Schulungsbedarfe durch die Beteiligten abgeleitet werden.

EnBW-CERT ist bestrebt, die etablierten Ansprechpartner in der EnBW (EnBW-Informationssicherheits-Community) über potenzielle ernste Schwachstellen auf dem Laufenden zu halten, und wird diese Community, wann immer möglich und wenn es dem EnBW-CERT angemessen erscheint, proaktiv über solche Schwachstellen informieren. Dies entbindet die Systemverantwortlichen allerdings nicht davon, dass diese sich ebenfalls um die Sicherheit ihrer Systeme eigenverantwortlich kümmern.

4.5 Zusammenarbeit, Interaktion und Offenlegung von Informationen

Zwar gibt es rechtliche und ethische Beschränkungen für den Informationsfluss aus dem EnBW-CERT, die zum großen Teil auch in der "EnBW-Informationssicherheitspolitik" aufgeführt sind und die alle eingehalten werden, jedoch erklärt EnBW-CERT seine Absicht, zum Geist der Zusammenarbeit beizutragen, den das Internet geschaffen hat.
Daher werden zwar durch das EnBW-CERT geeignete Maßnahmen ergriffen, um wo nötig die Identität von Angehörigen des Verantwortungsbereiches und anderen Betroffenen zu schützen, ansonsten aber werden Informationen frei ausgetauscht, um damit andere bei der Lösung oder Verhinderung von Sicherheitsvorfällen zu unterstützen.

In den nachstehenden Absätzen bezieht sich "betroffene Parteien" auf die rechtmäßigen Eigentümer, Betreiber und die entsprechenden EDV-Anlagen. Es bezieht sich nicht auf nicht autorisierte Benutzer, einschließlich anderweitig autorisierter Benutzer, die eine Einrichtung in einer nicht berechtigten Art und Weise nutzen; solche Eindringlinge können seitens des EnBW-CERT keine Vertraulichkeit erwarten. Ausnahme hierzu stellen bestehende gesetzliche Rechte auf Vertraulichkeit dar, die ein solcher Eindringling haben kann oder auch nicht. Diese werden selbstverständlich dort geachtet, wo sie bestehen.

Informationen, die zur Veröffentlichung in Betracht gezogen werden, werden wie folgt klassifiziert:

1. Private Nutzerinformationen sind Informationen über bestimmte Benutzer oder in einigen Fällen bestimmte Anwendungen, die aus rechtlichen, vertraglichen und/oder ethischen Gründen als vertraulich betrachtet werden müssen. Private Benutzerinformationen werden nicht in identifizierbarer Form außerhalb des EnBW-CERT veröffentlicht, es sei denn, dies ist unten vorgesehen. Wenn die Identität des Benutzers unkenntlich ist oder gemacht wurde, können die Informationen freigegeben werden, z. B., um eine Beispieldatei zu zeigen, wie sie von einem Eindringling geändert wurde, oder um einen bestimmten Social-Engineering-Angriff zu demonstrieren.

2. Eindringlingsinformationen ähneln privaten Benutzerinformationen, betreffen jedoch Eindringlinge. Während Eindringlingsinformationen, insbesondere identifizierende Informationen, nicht an die Öffentlichkeit freigegeben werden (es sei denn, sie werden öffentlich zugänglich, z. B. weil Strafanzeigen gestellt wurde), können diese im Rahmen der Vorfallsbehandlung mit betroffenen Systemadministratoren und CSIRTs ausgetauscht werden.

3. Private Website-Informationen sind technische Informationen über bestimmte Systeme oder Websites. Diese werden nicht ohne die Erlaubnis der Verantwortlichen der betreffenden Website freigegeben, außer wie unten vorgesehen.

4. Informationen zu Sicherheitsanfälligkeiten sind technische Informationen zu Sicherheitslücken oder Angriffen, einschließlich Patches und Mitigationsmaßnahmen („work-arounds"). Informationen über Sicherheitsanfälligkeiten werden frei veröffentlicht, obwohl alle Anstrengungen unternommen werden, um den jeweiligen Anbieter zu informieren, bevor die Öffentlichkeit informiert wird („responsible disclosure").

5. Zu den unangenehmen Informationen gehören die Aussage, dass ein Vorfall aufgetreten ist, sowie Informationen über seine Ausdehnung oder seinen Schweregrad. Unangenehme Informationen können eine Website oder einen bestimmten Benutzer oder eine bestimmte Benutzergruppe betreffen. Unangenehme Informationen werden nicht ohne die Erlaubnis der betreffenden Website oder der betreffenden Benutzer veröffentlicht, es sei denn, dies ist unten vorgesehen.

6. Statistische Informationen sind unangenehme Informationen, wobei die identifizierenden Informationen entfernt werden. Statistische Informationen werden nach Ermessen und in Abstimmung mit dem Leiter von C-TI veröffentlicht.

7. Kontaktinformationen sind Informationen, die es ermöglichen interne und externe Systemadministratoren und CSIRTs zu erreichen. Kontaktinformationen werden, wenn notwendig oder angebracht (z.B. im Rahmen eines Vorfalls), frei veröffentlicht, es sei denn, die Kontaktperson oder Einrichtung hat darum gebeten, dass dies nicht der Fall ist, oder wenn EnBW-CERT Grund zu der Annahme hat, dass die Verbreitung dieser Informationen nicht geschätzt werden würde.

Potenzielle Empfänger von Informationen aus dem EnBW-CERT werden wie folgt klassifiziert:

1. Mitglieder des EnBW-Aufsichtsrats, des EnBW-Vorstands, Mitglieder der Rechtsabteilung, der Chief Information Officer (CIO) sowie der Chief Information Security Officer (CISO) haben das Recht, alle von ihnen angeforderten Informationen zu einem IT-Sicherheitsvorfall (oder damit zusammenhängenden Fragen), der ihnen zur Abwicklung vorgelegt wurde, zu erhalten.

2. Aufgrund ihrer Verantwortung und der daraus resultierenden Erwartungen an die Vertraulichkeit haben Mitglieder des C-TI-Managements auf L1-Ebene oder höher das Recht, alle erforderlichen Informationen zu erhalten, um die Behandlung von IT-Sicherheitsvorfällen in ihren jeweiligen Zuständigkeitsbereich zu ermöglichen.

3. Mitglieder der EnBW Corporate Security Abteilung und des EnBW-CERT sind berechtigt (wenn ihre Beteiligung an einer Untersuchung eines Informationssicherheitsvorfall angefordert wurde bzw. wenn eine solche Untersuchung auf Anfrage von der EnBW Corporate Security oder des EnBW-CERT eingeleitet wurde), alle erforderlichen Informationen anzufordern, um die Durchführung von Ermittlungen und die Bearbeitung von Vorfällen in ihrem Zuständigkeitsbereich zu ermöglichen.

4. Systemadministratoren der EnBW oder EnBW IT erhalten vertrauliche Informationen, soweit dies für ihre Unterstützung bei einer Untersuchung notwendig oder zur Sicherung ihrer eigenen Systeme erforderlich ist.

5. Mitglieder der EnBW haben ein Anrecht auf Informationen, die sich auf die Sicherheit ihrer eigenen Computerkonten beziehen, auch wenn dies bedeutet, dass "Eindringlingsinformationen" oder "unangenehme Informationen" über einen anderen Nutzer offengelegt werden. Mitglieder der EnBW haben Anspruch darauf, benachrichtigt zu werden, wenn angenommen wird, dass ihr Konto kompromittiert wurde.

6. Kunden der EnBW oder externe Parteien sind nicht berechtigt, Informationen vom EnBW-CERT direkt anzufordern und zu erhalten. Die Übergabe von Informationen an Kunden oder Dritte erfolgt durch die Rechtsabteilung bzw. bei Kunden durch die Kundenschnittstelle (CRM). Das EnBW-CERT wird, nach der Überprüfung der Rechtmäßigkeit der Datenherausgabe, die erforderlichen Informationen zusammenstellen und diese gemäß Weisung bereitstellen.

7. Im Allgemeinen erhalten die Angehörigen des Verantwortungsbereiches des EnBW-CERT keine eingeschränkten Informationen, es sei denn, die betroffenen Parteien haben die Erlaubnis zur Verbreitung der Informationen erteilt.

   Statistische Informationen können den Angehörigen des Verantwortungsbereichs zur Verfügung gestellt werden.
   EnBW-CERT ist nicht verpflichtet, der Community alle Vorfälle zu melden, auch wenn sie sich dafür entscheiden kann. Insbesondere ist es wahrscheinlich, dass das EnBW-CERT entweder selbst alle direkt betroffenen Parteien über die Art und Weise informiert, in der sie betroffen sind, oder die betroffene Website dazu ermutigt, dies zu machen.

8. Generell werden keine eingeschränkten Informationen der allgemeinen Öffentlichkeit bereitgestellt. Das bedeutet, dass keine Anstrengungen unternommen werden, um mit der Öffentlichkeit zu kommunizieren. Das EnBW-CERT behandelt daher jede Information, die vom EnBW-CERT allgemein gegenüber Angehörigen der EnBW bekanntgegeben wird, als ob diese der allgemeinen Öffentlichkeit bekanntgegeben wird und passt deshalb die Informationen entsprechend an.

9. Die IT-Sicherheits-Community wird genauso behandelt wie die breite Öffentlichkeit. Mitglieder des EnBW-CERT können und werden an Diskussionen innerhalb der IT-Sicherheits-Community teilnehmen (z. B. Newsgroups, Mailinglisten (einschließlich vollständiger Offenlegungslisten wie z.B. bugtraq) sowie Konferenzen). Dabei werden sie die bei diesen Kreisen preisgegebenen Informationen so behandeln, als würden diese der allgemeinen Öffentlichkeit bekanntgegeben. Während technische Themen (einschließlich Schwachstellen) auf jeder Detailebene diskutiert werden können, werden alle Beispiele, die von innerhalb des Verantwortungsbereich des EnBW-CERT stammen, derart bereinigt, dass eine Identifizierung der betroffenen Parteien nicht möglich ist.

10. Die Presse wird auch als Teil der allgemeinen Öffentlichkeit betrachtet. EnBW-CERT wird nicht direkt mit der Presse in Bezug auf IT-Sicherheitsvorfälle interagieren, außer sie auf Informationen zu verweisen, die bereits von der EnBW der breiten Öffentlichkeit bereitgestellt wurden. Alle Anfragen, die sich auf Informationssicherheitsvorfälle beziehen, werden an die Abteilung für Pressearbeit der EnBW verwiesen.
    Bei Bedarf werden vom EnBW-CERT Informationen zusammengestellt und aufbereitet und dann den zuständigen Abteilungen der EnBW für Pressearbeit bzw. Kundenbeziehungsmanagement bereitgestellt.
    Unabhängig der obigen Einschränkungen, können die Mitglieder des EnBW-CERT, in Absprache mit der Pressestelle der EnBW, Interviews zu allgemeinen Fragen der Computersicherheit geben; in der Tat werden sie dazu auch ermutigt, dies als Teil des EnBW-Selbstverständnisses zu tun.

11. Im Rahmen von Untersuchungen von IT-Sicherheitsvorfällen werden in einigen Fällen vertrauliche Informationen mit externen Stellen und anderen CSIRTs geteilt. Dies geschieht nur, wenn die Vertrauenswürdigkeit und das berechtigte Interesse der externen Stellen überprüft werden können. Die übermittelten Informationen werden dabei so weit eingeschränkt, wie es im Rahmen der Untersuchungen bei der Bearbeitung eines Vorfalls hilfreich ist. Der Austausch solcher Informationen ist bei bekannten CSIRTs am wahrscheinlichsten (z. B. CERT-BUND).
    Zur Lösung eines Sicherheitsvorfalls gelten ansonsten halbprivate, aber relativ harmlose Nutzerinformationen wie die Herkunft von Verbindungen zu Nutzerkonten nicht als hochsensibel und können mit üblichen Vorsichtsmaßnahmen an eine fremde Stelle übertragen werden. "Eindringlingsinformationen" werden frei an andere Systemadministratoren und CSIRTs übermittelt. "Peinliche Informationen" können übermittelt werden, wenn hinreichende Gewähr dafür besteht, dass sie vertraulich bleiben, und wenn es notwendig ist, um einen Vorfall zu beheben.

12. Hersteller werden für die meisten Absichten und Zwecke als ausländische CSIRTs betrachtet. EnBW-CERT möchte Anbieter aller Arten von Netzwerk- und Computerausrüstung, Software und Dienstleistungen dazu ermutigen, die Sicherheit ihrer Produkte zu verbessern. Zu diesem Zweck wird eine in einem solchen Produkt entdeckte Sicherheitsschwachstelle, zusammen mit allen technischen Details, die zur Identifizierung und Behebung des Problems erforderlich sind, an den Hersteller gemeldet.
    Identifizierende Details werden dem Hersteller nicht ohne die Genehmigung der betroffenen Parteien, die die Schwachstellen entdeckt haben, mitgeteilt.

13. Die Strafverfolgungsbehörden werden vom EnBW-CERT, in Übereinstimmung mit den EnBW-Richtlinien und allen einschlägigen Gesetzen, die gebührende Zusammenarbeit erhalten, einschließlich aller Informationen, die sie benötigen, um eine Untersuchung durchzuführen. Die Koordination dieser Zusammenarbeit wird von der Rechtsabteilung der EnBW wahrgenommen. Die angeforderten Informationen werden vom EnBW-CERT der Rechtsabteilung zur Verfügung gestellt. Die Rechtsabteilung übergibt die Informationen an die Strafverfolgungsbehörden.

4.6 Kommunikation und Authentifizierung

Angesichts der Arten von Informationen, mit denen sich das EnBW-CERT wahrscheinlich befassen wird, werden Telefone als ausreichend sicher angesehen, um verwendet zu werden, selbst wenn sie keine Verschlüsselung des Sprachstroms anbieten.
Unverschlüsselte E-Mails gelten nicht als besonders sicher, sondern reichen nur für die Übertragung von Daten mit geringer Empfindlichkeit aus. Wenn es notwendig ist, hochsensible Daten per E-Mail zu senden, wird PGP, GPG oder S/MIME sowie gegebenenfalls auch andere Absicherungsmethoden (z.B. Microsoft Information Protection MIP) je nach Verfügbarkeit verwendet.
Netzwerkdateiübertragungen werden für diese Zwecke wie E-Mail betrachtet: Sensible Daten werden für die Übertragung verschlüsselt und auf eine Verschlüsselung der Netzwerkkommunikation geachtet.

Wenn es erforderlich ist, ein Vertrauensverhältnis mit einer bisher unbekannten Gegenstelle zu etablieren (z.B. bevor das EnBW-CERT wegen Informationen der Gegenstelle Maßnahmen ergreifen kann oder EnBW-CERT Informationen gegenüber der Gegenstelle offenlegt), wird sowohl die Identität und die Vertrauenswürdigkeit der unbekannten Gegenstelle überprüft, bis ein angemessenes Maß an Vertrauen festgestellt wurde.
Innerhalb der EnBW und bei bekannten externen Stellen reichen Empfehlungen von bekannten vertrauenswürdigen Personen aus, um jemanden zu authentifizieren und dadurch das notwendige Maß an Vertrauen herzustellen. Andernfalls werden geeignete Methoden verwendet (z.B. Suche nach FIRST-Mitgliedern, die Verwendung von WHOIS und anderen Internet-Registrierungsinformationen, zusammen mit einem telefonischen Rückruf oder einer Kontaktüberprüfung mittels signierter E-Mail), um sicherzustellen, dass die anfragende Gegenstelle vertrauenswürdig ist.
Daten, die per E-Mail an das EnBW-CERT übermittelt werden und denen vertraut werden muss, werden vom EnBW-CERT durch Kontakt mit dem Absender persönlich oder mittels digitaler Signaturen (PGP / GPG / S/MIME) überprüft.

5 Leistungsangebot

5.1 Reaktive Maßnahmen bei IT-Sicherheitsvorfällen

Das EnBW-CERT unterstützt federführend Verantwortliche und deren Systemadministratoren bei der operativen Abwicklung der technischen und organisatorischen Aspekte von IT-Sicherheitsvorfällen im Verantwortungsbereich des EnBW-CERT.
Das EnBW-CERT bietet dazu Unterstützung, Hilfestellungen sowie Beratung in den nachfolgenden Phasen des Vorfallmanagements:

5.1.1 Triage

- Untersuchen, ob tatsächlich ein Vorfall aufgetreten ist.
- Bestimmung des Ausmaßes des Vorfalls.
- Entscheidung der Vorgehensweise zur Vorfallsbehandlung

5.1.2 Koordinierung

- Ermittlung der ursprünglichen Ursache des Vorfalls, d. h. Identifizierung der vom Angreifer ausgenutzten Schwachstelle.
- Unterstützung bei der Kontaktaufnahme/Delegation mit/zu anderen externen Stellen, die involviert sein können.
- Unterstützung bei der Kontaktaufnahme/Delegation mit/zu internen Stellen der EnBW (z.B. Konzernsicherheit, Rechtsabteilung, Datenschutzbeauftragtem) und/oder gegebenenfalls entsprechenden Strafverfolgungsbehörden.
- Erstellen von Berichten an andere CSIRTs.
- Verfassen von Benachrichtigungen an betroffene Benutzer, falls zutreffend.

5.1.3 Vorfallsbehandlung

- Unterstützung/Beratung zur Behebung der Schwachstelle, wenn möglich.
- Sichern des Systems vor den Auswirkungen des Vorfalls.
- Bewertung, ob bestimmte Maßnahmen ausreichende Ergebnisse im Verhältnis zu ihren Kosten und Risiken bringen, insbesondere bei Maßnahmen, die auf eine eventuelle Strafverfolgung oder Disziplinarmaßnahme abzielen, wie z.B. Sammlung von Beweisen nach einem IT-Sicherheitsvorfall, Beobachtung eines Vorfalls im Gange, Einsatz von Honeypots.
- Das Sammeln von Beweisen, bei denen strafrechtliche Verfolgung oder Disziplinarmaßnahmen in Betracht gezogen werden.

Darüber hinaus sammelt das EnBW-CERT Statistiken zu Vorfällen, die innerhalb des definierten Verantwortungsbereich auftreten oder diesen betreffen, und informiert die Angehörigen des Verantwortungsbereiches bei Bedarf, um beim Schutz vor bekannten Angriffen zu helfen.
Um die Dienste des EnBW-CERT im Falle eines Vorfalls anzufordern, sollte, sofern noch keine Kontaktaufnahme durch das EnBW-CERT erfolgt ist, durch Eröffnung eines Sicherheitsincidents oder über den IT-Support bzw. ServiceCockpit (siehe Abschnitt 2.5) oder über die EnBW-CERT-E-Mailadresse (siehe Abschnitt 2.12) Unterstützung angefragt werden. Dabei muss beachtet werden, dass die verfügbare Unterstützung je nach den in Abschnitt 4.4 beschriebenen Vorgaben und Prioritäten variiert.

5.2 Proaktive Maßnahmen

EnBW-CERT koordiniert und bietet die folgenden Dienstleistungen, in Abhängigkeit der zur Verfügung stehenden Ressourcen („best-effort"), an.

5.2.1 Bereitstellung von Informationen und Lagebilderstellung

- Verteilung von für die EnBW relevanten Sicherheitshinweisen, die von überwachten Quellen für Informationssicherheits- und Schwachstellenwarnungen (z. B. BSI/US-CERT/US-CISA-Empfehlungen, veröffentlichte Sicherheitsinformationen von Herstellern) veröffentlicht wurden.
- Das EnBW-CERT bezieht Bedrohungsinformationen von verschiedenen Quellen und bewertet diese. Im Falle einer Relevanz für die Constituency des EnBW-CERT veröffentlicht das EnBW-CERT Sicherheitsinformationen über interne Kommunikationskanäle und Prozesse.
- Darüber hinaus nutzt das EnBW-CERT die ihm zur Verfügung stehenden Bedrohungsinformationen zur Erstellung eines aktuellen Bedrohungs-Lagebildes. Dieses fließt in die Meldungen des EnBW-CERT mit ein und wird unter anderem auch für weitere Maßnahmen genutzt, z.B. die Priorisierung von möglichen Maßnahmen zur Vorbereitung einer möglichen Gefahrenabwehr.
- Während die Aufzeichnungen von IT-Sicherheitsvorfällen vertraulich bleiben, werden regelmäßig statistische Berichte den interessierten und berechtigten Stellen in der EnBW zur Bewertung und Verbesserung der IT-Sicherheitsmaßnahmen zur Verfügung gestellt.

5.2.2 Schulungen

- Die Mitglieder des EnBW-CERT bieten regelmäßig Schulungen zu Themen der IT- und Informationssicherheit an. Diese Schulungen richten sich primär an die Angehörigen der EnBW IT und sofern Kapazitäten oder Bedarf besteht auch an die EnBW im Ganzen.

5.2.3 IT-Sicherheitsaudits

- Durchführung von Schwachstellenscans: Das EnBW-CERT kann eigene Schwachstellenscans durchführen bzw. auf die Ergebnisse der zentral durchgeführten Schwachstellenscans zugreifen, um dedizierte Systeme auf Schwachstellen bei Bedarf zu prüfen und frühzeitig Gegenmaßnahmen veranlassen zu können.
- Durchführung von IT-Sicherheitsaudits: Informationsverbünde und die durch diese bereitgestellten Dienste (wenn diese ein Bestandteil der in Abschnitt 3.5 definierten Netzwerke sind), die im Verantwortungsbereich der EnBW liegen, können auditiert werden, um deren aktuellen Reifegrad bezüglich der IT- und Informationssicherheit festzustellen.
  Diese Informationen zum Reifegrad des Sicherheitsniveaus werden interessierten und berechtigten Stellen in der EnBW zur Verfügung gestellt, um die Integration und Nutzung der bereitgestellten Dienste zu erleichtern. Einzelheiten der Sicherheitsanalysen werden jedoch vertraulich behandelt und nur den betroffenen Parteien zur Verfügung gestellt.
- Aufzeichnungen über behandelte Sicherheitsvorfälle werden gemäß den in den Abschnitten 4.2/4.3 aufgeführten Regelungen aufbewahrt.
  Während die Aufzeichnungen vertraulich bleiben, werden regelmäßig statistische Berichte interessierten und berechtigten Stellen in der EnBW zur Verfügung gestellt.

5.3 Weitere Leistungen

5.3.1 Kommunikation mit externen Stellen

- Das EnBW-CERT ist gegenüber dem BSI als meldende Stelle für KRITIS-Meldungen benannt. Daher erfolgt die Koordination und das Absetzen von entsprechenden Meldungen durch das EnBW-CERT.
- Ebenfalls ist das EnBW-CERT als Kommunikationspunkt für den Austausch mit dem Cyberversicherer für das Anzeigen eines (möglicherweise) eingetretenen Schadens zuständig sowie für die weitere Koordination im Rahmen der Vorfallsbehandlung des Versicherungsschadensfalles.
- Annahme von an das EnBW-CERT von Dritten gemeldeten Schwachstellen sowie Kommunikation und Koordinierung mit den meldenden Dritten und relevanten Stellen zur Behebung von diesen.

5.3.2 Beratungen zu Fragen der IT- und Informationssicherheit

- Die Mitglieder des EnBW-CERT führen Beratungen bei Projekten im Planungsstadium und auch etablierte Services zu Aspekten der IT- und Informationssicherheit sowie auch in gewissem Umfang zu technischen Datenschutzanforderungen durch. Bei komplizierteren Datenschutzthemen erfolgt eine Involvierung der Datenschutzverantwortlichen.

6 Formulare für die Meldung von Vorfällen

Vorfälle können über einen beliebigen Kommunikationskanal (gemäß Kapitel 2) an das EnBW-CERT gemeldet werden und müssen keine besondere Form erfüllen.

7 Haftungsausschlüsse

Während bei der Erstellung von Informationen, Benachrichtigungen und Warnungen jede Vorsichtsmaßnahme getroffen wird, übernimmt das EnBW-CERT keine Verantwortung für Fehler oder Auslassungen oder für Schäden, die sich aus der Verwendung der darin enthaltenen Informationen ergeben.