RFC 2350 - CSIRT der ERGO Group AG

Kontakt
CSIRT der ERGO Group AG

Tel.: +49 211 477 4700

Geltungsbereich
ERGO Group AG

Gültig ab
8. April 2024

Version
1.0

Klassifizierung
Öffentlich / public

Inhaltsverzeichnis

1. Informationen zum Dokument

Dieses Dokument enthält eine Beschreibung des ERGO Global IT Security Computer Incident Response Teams (CSIRT der ERGO Group AG) gemäß RFC 2350. Es enthält grundlegende Informationen über das CSIRT der ERGO Group AG, die Möglichkeiten zur Kontaktaufnahme und beschreibt die angebotenen Dienstleistungen.

1.1. Datum der letzten Aktualisierung

Das Dokument wurde zuletzt am 8. April 2024 aktualisiert.

1.2. Verteilerliste für Benachrichtigungen

Es sind keine Verteilerlisten für die Benachrichtigung über Aktualisierungen dieses Dokuments definiert.si.

1.3. Orte, an denen dieses Dokument gefunden werden kann

Die aktuelle Version der Beschreibung des CSIRT der ERGO Group AG ist verfügbar unter: https://www.ergo.com/de/Unternehmen/Corporate-Governance/Richtlinien-Regelwer

2. Kontaktinformationen

2.1. Name des Teams

CSIRT der ERGO Group.

2.2. Adresse

Die Besuchs- und Postanschrift lautet:
ERGO Group AG
ERGO-Platz 1
40477 Düsseldorf
Deutschland

2.3. Zeitzone

UTC+2h (MESZ) Sommerzeit zwischen dem letzten Sonntag im März und dem letzten Sonntag im Oktober. UTC+1h (MEZ) sonst.

2.4. Telefon Nummer

+49 211 477 4700.

2.5. Fax-Nummer

Keine.

2.6. Sonstige Telekommunikation

Keine.

2.7. Elektronische Postadresse

csirt@itergo.com

2.8. Informationen zur Verschlüsselung

Falls ein vertraulicher Austausch erforderlich ist, schreiben Sie bitte eine E-Mail mit der Bitte um einen Schlüsselaustausch (siehe 2.7).

2.9. Teammitglieder

Es werden keine Informationen an die Öffentlichkeit gegeben.

2.10. Andere Informationen

Keine.

2.11. Kontaktstellen für Kunden

Die Betriebszeiten sind generell auf die Geschäftszeiten beschränkt: Mo-Fr, 9.00 - 17.00 Uhr MEZ/MESZ. Der bevorzugte Weg zur Kontaktaufnahme mit dem CSIRT der ERGO Group AG ist eine E-Mail an csirt@itergo.com. In dringenden Fällen kann das CSIRT der ERGO Group AG unter der Hotline in Kapitel 2.4 erreicht werden (24/7).

3.Charta

3.1. Leitbilder

Das CSIRT der ERGO Group AG hat die Aufgabe, die Aktivitäten in Bezug auf IT-Sicherheitsvorfälle für den in Kap. 3.2 definierten Personenkreis zu koordinieren und zu betreiben, um potenzielle Risiken zu vermeiden oder zu reduzieren.

3.2. Wahlkreis

Die Dienste stehen der ERGO Group AG und ihren Tochtergesellschaften zur Verfügung. Das CSIRT der ERGO Group AG ist für die ASN AS28674 zuständig.

3.3. Sponsoring und/oder Zugehörigkeit

Das CSIRT ist Teil der ERGO Group AG und seinen Tochterunternehmen.

3.4. Zuständigkeit

Der Hauptzweck des CSIRT der ERGO Group AG besteht in der gruppenweiten und multinationalen Koordinierung der Reaktion auf Sicherheitsvorfälle und der operativen Bearbeitung von Sicherheitsvorfällen im Namen und/oder auf Ersuchen seiner Mitglieder (siehe Kap. 3.2).

4.Leitlinien

4.1. Arten von Vorfällen und Umfang der Unterstützung

Die Aufgaben des CSIRT der ERGO Group AG umfassen die proaktive und reaktive Bearbeitung aller möglichen Arten von IT-Sicherheitsvorfällen. Der Beginn der Reaktionsmaßnahmen richtet sich nach der Schwere der Auswirkungen des Sicherheitsvorfalls.

4.2. Zusammenarbeit, Interaktion und Offenlegung von Informationen

Das CSIRT der ERGO Group AG arbeitet mit den zuständigen Behörden und Regulierungsstellen zusammen und interagiert mit vertrauenswürdigen CSIRTs auf nationaler und internationaler Ebene, wo dies als nützlich erachtet wird, vor allem durch den Austausch von Erfahrungen und bewährten Verfahren. Diese Art der Zusammenarbeit kann auch den Austausch von Informationen über Sicherheitsvorfälle und Schwachstellen umfassen. Das CSIRT der ERGO Group AG schützt stets die Privatsphäre seiner Partner und Kunden und verarbeitet die Informationen in Übereinstimmung mit den Beschränkungen des deutschen Bundesdatenschutzgesetzes (BDSG) und der EU-Datenschutzgrundverordnung (GDPR).

4.3. Kommunikation und Authentifizierung

Das Information Sharing Traffic Light Protocol (ISTLP) wird auf alle Informationen angewandt, die zwischen dem CSIRT der ERGO Group AG und anderen CSIRTs ausgetauscht werden, unabhängig von den Kommunikationsmedien (z. B. E-Mail, Telefon oder persönliche Treffen). Der Austausch vertraulicher Informationen erfolgt nach dem Verfahren in Kapitel 2.8.

5. Dienstleistungen

5.1. Triage von Vorfällen

- festzustellen, ob ein gemeldeter Vorfall authentisch und echt positiv ist
- festzustellen, welche Bestandteile betroffen sind oder betroffen sein könnten
- den Vorfall zu bewerten und Prioritäten zu setzen

5.2. Reaktion auf Vorfälle

- Leitung des Verfahrens zur Reaktion auf Sicherheitsvorfälle
- sicherstellen, dass auf Sicherheitsvorfälle angemessen reagiert wird, und bei Bedarf Unterstützung bei der Schadensbegrenzung leisten
- Kontaktaufnahme mit den betroffenen Organisationen, um mit ihnen zusammenzuarbeiten und sie zu informieren, damit sie die entsprechenden Maßnahmen ergreifen
- Einrichtung von Kommunikationskanälen und Übermittlung der erforderlichen Informationen an die zuständigen Stellen bei Sicherheitsvorfällen

5.3. Digitale Forensik

- Protokollanalyse
- Speicherforensik
- Forensik physischer/virtueller Laufwerke
- Netzwerk-Forensik
- Malware-Analyse

6. Formulare zur Meldung von Vorfällen

Vorfälle können über die in diesem Dokument genannten Kommunikationskanäle (2.4 und 2.7) gemeldet werden und müssen keiner bestimmten Form entsprechen.

7. Haftungsausschlüsse

Obwohl alle Vorsichtsmaßnahmen bei der Erstellung von Informationen, Meldungen und Warnungen getroffen werden, übernimmt das CSIRT der ERGO Group AG keine Verantwortung für Fehler oder Auslassungen oder für Schäden, die sich aus der Verwendung der darin enthaltenen Informationen ergeben.