ThüringenCERT Beschreibung nach RFC 2350

1. Vorbemerkung

Dieses Dokument beschreibt in Anlehnung an RFC 2350 (Expectations for Computer Security Incident Response, http://www.ietf.org/rfc/rfc2350.txt) die technische und organisatorische Schnittstelle zum ThüringenCERT, dem „Computer Emergency Response Team“ für die Thüringer Landesverwaltung. Eine formalisierte Kurzdarstellung einer CERT-Struktur nach RFC 2350 hat sich als quasi-Standard etabliert und ist geeignet, um sich einen schnellen Überblick über die Schnittstellen und Dienstleistungen eines CERT zu verschaffen.

Eine aktuelle Fassung kann heruntergeladen werden unter:

https://landesrechenzentrum.thueringen.de/it-landesdienstleister/cert/

2. Kontaktdaten

2.1 Name des Teams

ThüringenCERT

2.2 Postalische Adresse

Thüringer Landesrechenzentrum
Referat 25 ThüringenCERT
Ludwig-Erhard-Ring 8
99099 Erfurt

2.3 Zeitzone:

Europa/Berlin, GMT+1 und Europa/Berlin, GMT+2 gemäß § 2 SoZV vom letzten Sonntag im März bis zum letzten Sonntag im Oktober

2.4 Telefon

+49 361 57-101

2.5 Fax

+49 361 57-3635848

2.6 E-Mail

cert@tlrz.thueringen.de

2.7 Public Keys und Informationen zur Signierung und Verschlüsselung

Für die elektronische Übermittlung vertraulicher Informationen wird die Nutzung von S/MIME- oder PGP-Verschlüsselung empfohlen. Unterstützt werden S/MIME, PGP und Chiasmus.

Folgender öffentlicher PGP-Schlüssel gilt zurzeit:
ID: 5AF2EB58
Fingerprint: A2F7 CB4C B282 5142 5D8D 3E4C 9411 6C4F 5AF2 EB58

Der öffentliche PGP-Schlüssel steht zum Download bereit unter:
https://landesrechenzentrum.thueringen.de/fileadmin/th5/tlrz/public_key_thueringencert.txt

Es wird empfohlen, den Fingerprint telefonisch zu verifizieren.
S/MIME Fingerprint: 1CD6 903B 2527 4A03 B68A E62E 3F39 7712 2A77 2F84
Der Schlüssel für Chiasmus wird auf Anfrage vertraulich bereitgestellt.

2.8 Personelle Zusammensetzung des ThüringenCERT

Die Mitarbeiterinnen und Mitarbeiter des ThüringenCERT sind Bedienstete des Thüringer Landesrechenzentrums (TLRZ).

2.9 Betriebszeiten

Die bevorzugte Kontaktaufnahme soll über E-Mail erfolgen.

Montags-Donnerstags: 08:00 Uhr bis 16:00 Uhr
Freitags: 08:00 Uhr bis 15:00 Uhr
(Ausnahmen: 24. und 31. Dezember sowie gesetzliche Feiertage in Thüringen)

3. Organisatorischer Rahmen

3.1 Ziele und Aufgaben (Mission Statement)

Das ThüringenCERT ist eine Organisationseinheit, die zur Prävention und Bearbeitung von Informationssicherheitsvorfällen sowie zur allgemeinen Erhöhung der Qualität der Informationssicherheit der Landesverwaltung des Freistaats Thüringen dient.

Entsprechend der Informationssicherheitsleitlinie der Thüringer Landesverwaltung, nimmt das Thüringen insbesondere folgende Aufgaben wahr:

- Betrieb eines Warn- und Informationsdienstes für die Thüringer Landesverwaltung
- Koordinierende Bearbeitung von bedeutsamen Sicherheitsvorfällen
- Erstellung von Handlungsempfehlungen für betroffene Stellen
- Unterstützung der Aufgabenerfüllung der Informationssicherheitsbeauftragten (ISB) der Thüringer Landesverwaltung

Das ThüringenCERT ist die zentrale Kontaktstelle für Meldungen von Angriffen und Sicherheitsvorfällen.

3.2 Zielgruppe (Constituency)

Zielgruppe des ThüringenCERT sind alle Behörden und Einrichtungen der Landesverwaltung des Freistaats Thüringen.

Innerhalb der angesprochenen Behörden und Organisationseinheiten richten sich die Dienstleistungen des ThüringenCERT primär an die jeweils verantwortlichen ISB.

3.3 Domänen und IP-Adressbereiche

Das ThüringenCERT ist zuständig für das Netz der Thüringer Landesverwaltung (AS 196870)

Ipv4 Adressbereich: 195.191.14.0/23

IPv6 Adressbereich: 2001:67c:cc::/48

Domains: sämtliche Domains die auf das genannte Netz auflösen (u. a. *.thueringen.de).

3.4 Betrieb

Das ThüringenCERT ist beim Thüringer Landesrechenzentrum (TLRZ) angesiedelt.

3.5 Zuständigkeiten und Befugnisse (Authority)

Das ThüringenCERT arbeitet primär für die Landesverwaltung und unter der Fach- und Dienstaufsicht des Thüringer Finanzministeriums.

Das ThüringenCERT ist autorisiert, alle Angriffe auf und Sicherheitsvorfälle innerhalb der Thüringer Landesverwaltung zu bearbeiten und zu koordinieren. Die angebotene Unterstützung ist primär auf die Thüringer Landesverwaltung und bei Vorfällen involvierten Parteien begrenzt.

Alle Informationen, von denen das ThüringenCERT im Rahmen seiner Aufgabenerfüllung Kenntnis erlangt, werden mit größter Sorgfalt behandelt und unter gebührender Wahrung der Vertraulichkeit. Das ThüringenCERT richtet sich grundsätzlich nach dem international normierten „Information Sharing Traffic Light Protocol“ (ISTLP)[1]. Informationen, die mit einer entsprechenden Kennzeichnung versehen sind, werden entsprechend behandelt, sofern dem keine dienstlichen Vorschriften entgegenstehen.

Das ThüringenCERT verwendet für sensitive oder sicherheitskritische Informationen eine verschlüsselte Kommunikationsform. Dies gilt besonders für Informationen, die als „TLP AMBER“ oder „TLP RED“ eingestuft werden.

3.6 Dienstleistungen (Services)

Reaktive Dienstleistungen

Das ThüringenCERT ist verantwortlich für die Bearbeitung

- von Sicherheitsvorfällen innerhalb der Zielgruppe
- Reaktion auf Angriffe auf die Zielgruppe
- der Information der Betroffenen und
- die Koordinierung der Reaktion sowie weiterer Schutzmaßnahmen.

Insbesondere wird durch das ThüringenCERT gewährleistet, dass die verantwortlichen Stellen der Landesverwaltung zeitnah über Entwicklungen und Lagen informiert werden.

Präventive Dienstleistungen

Das ThüringenCERT betreibt einen Warn- und Informationsdienst, um bei Sicherheitslücken in IT-Systemen aktuellen Bedrohungen und Angriffen die Zielgruppe zeitnah zu informieren.

Ebenso ist das ThüringenCERT in das Informationssicherheitsmanagement der Thüringer Landesverwaltung eingebunden, unterstützt die für Informationssicherheit verantwortlichen Stellen und trägt zu einer kontinuierlichen Verbesserung der Informationssicherheit innerhalb der Zielgruppe bei.

3.7 Meldung von Angriffen und Vorfällen

Für die Meldung von Sicherheitsvorfällen und Angriffen wird eine vertrauliche Übermittlung per verschlüsselter E-Mail empfohlen. Damit eine weitere Bearbeitung erfolgen kann, ist es zwingend erforderlich, dass die Kontaktdaten zur eigenen Person und Einrichtung vollständig und aktuell sind.

Die verantwortlichen Betreiber von IT-Infrastrukturen in der Landesverwaltung geben informationssicherheitsrelevante Informationen über geeignete IT-Systeme an das ThüringenCERT weiter. Meldewürdig sind dabei vor allem Ereignisse, bei denen Auswirkungen auf andere nicht ausgeschlossen werden können, oder die auch für andere als relevant eingeschätzt werden, z. B. besondere Auffälligkeiten und klare Abweichungen vom Normalverhalten im Regelbetrieb.

Für eine korrekte und vollständige Erfassung und geeignete Priorisierung von Informationssicherheitsvorfällen sind uns nach Möglichkeit mindestens die folgenden Informationen zu übermitteln:

Kontaktdaten der meldenden Person

- Meldende Organisation/Behörde
- Name und Funktion der meldenden Person
- Standort / Postanschrift der Organisation / Behörde
- Telefonische Kontaktdaten für kurzfristige Rückfragen
- E-Mail-Adresse der meldenden Person

[1] https://www.trusted-introducer.org/ISTLPv11.pdf

Angabe des Ressorts / der Abteilung / des Teams, in dem der Vorfall entdeckt worden ist

Art der Meldung (Erst-, Zwischen- oder Abschlussmeldung)

Einstufung des Vorfalls aus Sicht der meldenden Organisation:

- Sind Schäden entstanden oder drohen akut?
- Wie schwer sind die entstandenen oder drohenden Schäden?
- Dringlichkeit

Technische Angaben zum festgestellten Informationssicherheitsvorfall:

- Was ist passiert?
- Wann ist es passiert?
- Wann wurde es entdeckt?
- Wie wurde es entdeckt?
- Welche Maßnahmen wurden bereits eingeleitet?
- Welche Schäden und Auswirkungen wurden festgestellt oder sind möglich?

Für Meldungen von Informationssicherheitsvorfällen innerhalb der Thüringer Landesverwaltung stellen wir ein Meldeformular auf unserer Intranet Seite zur Verfügung, welches alle diese Informationen strukturiert erfasst.

3.8 Haftungsausschluss

Die Aufbereitung von Informationen, Benachrichtigungen und Warnungen erfolgt mit der gegebenen Sorgfalt, jedoch übernimmt das ThüringenCERT keine Verantwortung für Fehler, Auslassungen oder für Schäden aus der Nutzung der darin enthaltenen Informationen.