STAATSBETRIEB
SÄCHSISCHE
INFORMATIK DIENSTE

Freistaat
SACHSEN

Informationen über SAX.CERT im RFC2350-Format

1 Über dieses Dokument

1.1 Datum der letzten Änderung

Version 1.3 vom 3. Januar 2018

1.2 Informationen über neue Versionen

Email-Benachrichtigungen über neue Versionen werden an den deutschen Verwaltungs-CERT-Verbund, den allgemeinen deutschen CERT Verbund und den Trusted Introducer Service für Incident-Response-Teams und Sicherheitsteams (https://www.trusted-introducer.org) weitergegeben.

1.3 Verteilung des RFC 2350

Diese aktuelle Version der Informationen wird intern im SID verwendet und auf der Web-Site http://www.cert.sachsen.de veröffentlicht.

1.4 Rückfragen

Alle Fragen bzgl. dieses Dokuments und bzgl. des SAX.CERT sind per Email an sax.cert@cert.sachsen.de zu richten.

2 Kontaktinformationen

2.1 Name des Teams

Voller Name: SAX.CERT

Kurzname: SAX.CERT

2.2 Adresse

Postanschrift:

Staatsbetrieb Sächsische Informatik Dienste
z. Hd. SAX.CERT-Team
Riesaer Str. 7
01129 Dresden
Germany

2.3 Zeitzone

GMT01 / GMT02 (DST)

2.4 Telefon

+49 351 7999 77 99

2.5 Fax

+49 351 84732396

ACHTUNG: Krypto-FAX. Bitte vor Versand +49 351 7999 77 99 anrufen.

2.6 Andere Telekommunikation

+49 351 84732396

ACHTUNG: Krypto-FAX. Bitte vor Versand +49 351 7999 77 99 anrufen.

2.7 Email

Berichte über Vorfälle und sicherheitskritische Ereignisse senden Sie bitte per Email an sax.cert@cert.sachsen.de

2.8 Kryptographisches Schlüsselmaterial

2.8.1 PGP/GnuPG

Aktuell gültig ist der folgende Schlüssel:

0xA478B1C2 SAX.CERT <sax.cert@cert.sachsen.de>

Fingerprint: 40C3 7E86 5A3E 9C61 5D25 7B1C A814 30A3 A478 B1C2

Der öffentliche Schlüssel wird auf allgemein zugänglichen PGP-Keyservern (z.B. keyserver.pgp.com) bereitgestellt.

2.8.2 S/MIME

Das aktuell gültige X.509 Zertifikat für sax.cert@cert.sachsen.de lautet:


```
-----BEGIN CERTIFICATE-----
MIIGFDCCBPygAwIBAgIHGZjFqHWZpjANBgkqhkiG9w0BAQsFADCBwDELMAkGA1UE
BhMCREUxEDAOBgNVBAgTB1NhY2hzZW4xEDAOBgNVBAcTB0RyZXNkZW4xGjAYBgNV
BAoTEUZyZWlzdGFhdCBTYWNoc2VuMTIwMAYDVQQLEylTYWVjaHNpc2NoZXMgU3Rh
YXRzbWluaXN0ZXJpdW0gZGVzIEludmVybjEaMBgGA1UEAxMRU2FjaHNlbiBHbG9i
YWwgQ0ExITAfBgkqhkiG9w0BCQEWEnBraUBzbWkuc2FjaHNlbi5kZTAeFw0xNTA2
```

MTEwODM0MzJaFw0xODA2MTAwODM0MzJaMHwxCzAJBgNVBAYTAkRFMRowGAYDVQQK
DBFGcmVpc3RhYXQgU2FjaHNlbjE1MDMGA1UECwwsU3RhYXRzYmV0cmllYiBTYWVj
aHNpc2NoZSBJbmZvcm1hdGlrIERpZW5zdGUxGjAYBgNVBAMMEUdSUDogQ0VSVCBT
YWNoc2VuMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqOhde6CKTGgh
bEXjpEPaUfzgRl2TxZs0F37LJ6ia+NJOAzLJFDh/k/CU313Bx9bZRff8YgoWXcok
/jZOi87DytKAn/nWPnrfWMd+UF46hLs1yN7gfiOKfl2PsEAEJZkkm6MDJiVodsoN
ZoGzyunF8mKRP7ZtIkcqEy+BG3jwzYLIQe9mueBsTg4Q/o3TjgQXItXfa7kxtNZq
HPExp+DlUxSLboD6pCRyoqgsw3MOOmCcO/XjZSHLjC4dMs8vLLFJUsewU/jeYxDk
khn0QZ83buQPZJ5jcVn3GsAuiSLItZeoZ32iInMLOwgzaRoHidQgXXtanEx/GUtr
pKTehPtk1wIDAQABo4ICVDCCAlAwQAYDVR0gBDkwNzARBg8rBgEEAYGtIYIsAQEE
AwMwEQYPKwYBBAGBrSGCLAIBBAMBMA8GDSsGAQQBga0hgiwBAQQwCQYDVR0TBAIw
ADALBgNVHQ8EBAMCBeAwHQYDVR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMEMB0G
A1UdDgQWBBStrw0KybehwVFA7VKefLxBIKZtdjAfBgNVHSMEGDAWgBTNzv6x//ku
5Jap/yvjLYAdjkqY9TAjBgNVHREEHDAagRhzYXguY2VydEBjZXJ0LnNhY2hzZW4u
ZGUwgY8GA1UdHwSBhzCBhDBAoD6gPIY6aHR0cDovL2NkcDEucGNhLmRmbi5kZS9z
YWNoc2VuLWdsb2JhbC1jYS9wdWIvY3JsL2NhY3JsLmNybDBAoD6gPIY6aHR0cDov
L2NkcDIucGNhLmRmbi5kZS9zYWNoc2VuLWdsb2JhbC1jYS9wdWIvY3JsL2NhY3Js
LmNybDCB3QYIKwYBBQUHAQEEgdAwgc0wMwYIKwYBBQUHMAGGJ2h0dHA6Ly9vY3Nw
LnBjYS5kZm4uZGUvT0NTUC1TZXJ2ZXIvT0NTUDBKBggrBgEFBQcwAoY+aHR0cDov
L2NkcDEucGNhLmRmbi5kZS9zYWNoc2VuLWdsb2JhbC1jYS9wdWIvY2FjZXJ0L2Nh
Y2VydC5jcnQwSgYIKwYBBQUHMAKGPmh0dHA6Ly9jZHAyLnBjYS5kZm4uZGUvc2Fj
aHNlbi1nbG9iYWwtY2EvcHViL2NhY2VydC9jYWNlcnQuY3J0MA0GCSqGSIb3DQEB
CwUAA4IBAQAIUEgqZd9h38GHDA63K9YsTRpsyiXGiA8k69vGNJu3VvVxzH0NpeTv
iOeWl9XLyV+frCjp3zCnbjcrKmLBFdAyXFrfwu20dkEMysDP6GeNXBs+n+ZDvD3m
8S6icXONzPp/9zZ3NpJrr5w/PmaoyR71+YIgiXmc+XllQCE/4KCbI780Jm6ayKXY
YwEBoI/KKdGYBpTnvvcv/UTO/9xBQGtUuaQjocKEiPicYpSRRZH1/f6lSeWpD1jf
G3RCDNI0HnZUs2RiWXSYriSC2s7FpldeNnXqnxTBzUtbz/Gb5Iypm+RcvZFc17wd
DRdajHnWfWMlcjl/kKtcxSdocGiVbCzW
-----END CERTIFICATE-----

Der vollständige Zertifizierungspfad kann unter <Link> heruntergeladen werden.

2.9 Teammitglieder

Der Teamleiter ist:

Christoph Damm

Email: christoph.damm@sid.sachsen.de
Telefon: +49 351 3264 6630

Die Liste der Teammitglieder wird nicht veröffentlicht.

2.10 Bevorzugte Kontaktaufnahme

Die bevorzugte Kontaktaufnahme soll über Email erfolgen:

- Für Beschwerden über Spam etc. (Abuse): sax.cert@cert.sachsen.de
- Für aktuelle Vorfälle und Angriffe: sax.cert@cert.sachsen.de
- Für andere Anfragen und Informationen: sax.cert@cert.sachsen.de

Für die Übermittlung vertraulicher Informationen kann sowohl PGP/GnuPG als auch SMIME verwendet werden.

Eingehende Email wird während der Geschäftszeiten regelmäßig gesichtet und bearbeitet:

Montag bis Freitag zwischen 08.30 – 16.30 Uhr

Nicht an bundeseinheitlichen Feiertagen bzw. Feiertagen des Freistaats Sachsen.

3 Organisatorischer Rahmen

3.1 Ziel des Teams

SAX.CERT ist das Verwaltungs-CERT für alle obersten Landesbehörden des Freistaats Sachsen und diesen untergeordneten Behörden und Ämter bzw. öffentlichen Einrichtungen.

Besondere Aufgaben des SAX.CERT – gemäß VwV Informationssicherheit vom 07.09.2011, Punkt 4.3 Sicherheitsnotfallteam – sind:

- das Aufzeigen von Lösungen bei konkreten Sicherheitsvorfällen,
- die Mitwirkung als koordinierende Instanz für Informationssicherheit,
- die Information zu Sicherheitslücken und
- die Unterstützung zur Beseitigung von Sicherheitsrisiken.

Außerdem ist das SAX.CERT Ansprechpartner der Beauftragten für Informationssicherheit (BfIS) bei technischen Fragen zur Informationssicherheit.

In nationalen und internationalen CERT-Verbünden ist das SAX.CERT die Kontaktstelle für andere CERT und Meldungen über Angriffe und Sicherheitsvorfälle.

3.2 Zielgruppe

SAX.CERT ist das Verwaltungs-CERT für alle obersten Landesbehörden des Freistaats Sachsen und diesen untergeordneten Behörden und Ämter bzw. öffentlichen Einrichtungen.

3.3 Betrieb

Das SAX.CERT ist beim Staatsbetrieb Sächsische Informatik Dienste (SID) angesiedelt.

3.4 Autorität

Das SAX.CERT arbeitet im Ressortbereich und unter der Aufsicht des Sächsischen Staatsministeriums des Inneren.

4 Vorgaben und Verfahren

4.1 Arten von Vorfällen und angebotene Unterstützung

SAX.CERT ist autorisiert, alle Angriffe auf und Vorfälle innerhalb der betreuten Zielgruppe (siehe 3.2) zu bearbeiten und zu koordinieren.

Eine direkte, insbesondere telefonische, Unterstützung wird im Allgemeinen nur Personen gewährt, die durch den Freistaat beschäftigt sind bzw. für diesen tätig sind.

4.2. Weitergabe von Informationen

Alle Informationen, die durch das SAX.CERT bearbeitet werden, werden unabhängig von ihrer zeitlichen Priorität mit größter Sorgfalt behandelt und verarbeitet. Der Vertraulichkeit kommt hierbei eine große Bedeutung zu.

Um die Arbeit des SAX.CERT zu unterstützen ist es deshalb wichtig, bestehende Restriktionen oder Sensitivitäten direkt und unmittelbar anzusprechen, damit dies bei der weiteren Verarbeitung berücksichtigt werden kann.

Das SAX.CERT beachtet das international normierte sogenannte Information Sharing Traffic Light Protocol (ISTLP – siehe https://www.trusted-introducer.org/ISTLPv11.pdf). Informationen, die mit einer entsprechenden Angabe versehen sind (ISTLP: WHITE = frei von Beschränkungen, GREEN = öffentlich, AMBER = nur für Betroffene bzw. RED = nur SAX.CERT), werden entsprechend behandelt, sofern keine dienstlichen Vorschriften dem entgegenstehen.

4.3 Sicherung der Kommunikation

Bitte verwenden Sie für sensitive oder sicherheitskritische Informationen eine verschlüsselte Kommunikationsform. Dies gilt besonders für Informationen, die als ISTLP AMBER oder ISTLP RED eingestuft werden.

5 Dienste

5.1 Vorfallsbearbeitung

Das SAX.CERT ist für die Bearbeitung von Vorfällen innerhalb bzw. Angriffen auf die Zielgruppe verantwortlich für die Information der Betroffenen und die Koordinierung der Reaktion sowie weiterer Schutzmaßnahmen. Insbesondere wird durch das SAX.CERT gewährleistet, dass die verantwortlichen Stellen zeitnah über Entwicklungen und Lagen informiert werden.

5.2. Vorbeugende Aktivitäten

SAX.CERT führt folgende Aktivitäten durch, um die Sicherheit innerhalb der Zielgruppe stetig zu verbessern und die für Informationssicherheit verantwortlichen Stellen zu unterstützen:

- Frühwarnung und Schwachstellenwarnungen
- Informationsverteilung und Aufklärung
- Auswertung und Lagebild

6 Muster für Meldungen bei Angriffen und Vorfällen

Informationen des SAX.CERT über die Meldung bei Angriffen bzw. Vorfällen oder anderen sicherheitskritischen Vorkommnissen werden zukünftig auf den Web-Seiten des Teams veröffentlicht:

http://www.cert.sachsen.de

Für die Meldung wird eine vertrauliche Übermittlung per verschlüsselter E-Mail empfohlen.

Für die weitere Bearbeitung ist es zwingend erforderlich, dass die Angaben zur eigenen Person und Einrichtung vollständig und aktuell sind. Je mehr Informationen über Angriffe und Vorfälle verfügbar sind, desto besser und schneller kann die weitere Bearbeitung erfolgen. Besonders wichtig sind Angaben zu:

- Art des Vorfalls, Angaben zur technischen Vorgehensweise (Spam, Malware, Scanning, etc.)
- Genaue Zeit- und Datumsangaben, auch für Log-Dateien. Hierbei kann im Einzelfall auch die Zeitzone, die z.B. auf einem Server eingestellt ist, entscheidend für die richtige Auswertung sein.

Wenn Malware auf betroffenen Systemen vorgefunden wird und an das SAX.CERT übermittelt werden soll, muss individuell abgesprochen werden, wie die Übermittlung erfolgen kann, ohne das die installierten Anti-Virus-Filter bzw. angriffserkennenden Systeme dies verhindern oder Alarm auslösen.