Rahmenplan zur wöchentlichen CSCC-Telefonkonferenz

Termin	Inhalt	Verantwortlich
bis Do 12:00	Meldung von Sicherheitsvorfällen der vorigen Woche an TÜV TRUST IT[1]	CSCC-Mitglieder
bis Do 18:00	Aufbereitung und Konsolidierung der gemeldeten Sicherheitsvorfälle	TÜV TRUST IT
bis Fr 09:30	Versand der Einwahldaten und ggf. Hintergrund-informationen	TÜV TRUST IT
Fr 10:00–12:00	CSCC-Telefonkonferenz Einwahl:..... +49 69 2108 69 700 Teilnehmercode: (wird am Vormittag verschickt)	alle
Fr 12:00–14:00	Möglichkeit für individuelle telefonische Beratung bzw. Nachfragen	TÜV TRUST IT
Anschließend (Fr. oder Mo.)	Zusendung des Berichts und des Protokolls an die CSCC-Mitglieder	TÜV TRUST IT

[1] S/MIME- oder GnuPG-verschlüsselt an cscc@it-tuv.com
S/MIME-Fingerprint: 5163c0a1 b037025e 26ed1d45 62edf557 326ee50f
GnuPG-KeyID: 759B ABB7 21E6 A0F5 5E2F FDC0 0D09 E091 2F9E 3E57

Agenda zur wöchentlichen CSCC-Telefonkonferenz

Einwahl: .....+49 69 2108 69 700

Admincode: .....[über das Konferenzportal erstellt und bis 09:30h versandt]

Teilnehmercode:.[über das Konferenzportal erstellt und bis 09:30h versandt]

TOP	Inhalt	Verantwortlich
0	Begrüßung, Vollzähligkeit ggf. Vorstellung neuer Teilnehmer	TÜV TRUST IT
1	Offene Punkte der Vorwoche Sofern aus vergangenen Telefonkonferenzen noch offene Punkte zur Klärung vorliegen, werden diese hier besprochen.	TÜV TRUST IT
2	TÜV Case der Woche Eine aktuelle Entwicklung aus dem Umfeld der IT-Sicherheit wird vorgestellt, Hintergründe und Zusammenhänge erläutert und Auswirkungen und mögliche Mitigationsstrategien gegeben.	TÜV TRUST IT
3	Aktuelle Sicherheitslage Die wesentlichen, seit der letzten Telefonkonferenz aufgetretenen externen Ereignisse mit Bezug zur IT-Sicherheitslage werden kurz vorgestellt, im Hinblick auf ihre Relevanz bewertet und erste resultierende Handlungsempfehlungen für die CSCC-Teilnehmer ausgesprochen.	TÜV TRUST IT
4	Auswertung gemeldeter Sicherheitsvorfälle Die in der vergangenen Woche aufgetretenen Sicherheitsvorfälle werden in anonymisierter und konsolidierter Form vorgestellt und erste resultierende Handlungsempfehlungen für die CSCC-Teilnehmer ausgesprochen	TÜV TRUST IT sowie ggf. weitere Experten
5	Diskussion und Rückfragen Beantwortung bzw. Sammlung weiterer Rückfragen	alle

Im Nachgang zur wöchentlichen Telefonkonferenz besteht die Möglichkeit, individuelle Rücksprache zu Sicherheitsthemen in individuellen Telefonterminen wahrzunehmen.

CSCC Case der Woche

2016-01-01: Crypto-Ransomware „Ransom32“

Titel **Crypto-Ransomware „Ransom32“**	Risiko ■■■■□
Betroffene Systeme:	primär Windows potenziell alle Betriebssysteme
Sachstand:	Die Ransomware „Ransom32“ ist der erste weit verbreitete Krypto-Trojaner auf JavaScript-Basis.[1] Ransom32 gehört zu der Kategorie *Ransomware as a Service* und ist vergleichbar beispielsweise mit Tox[2]. Zur Nutzung des Dienstes wird lediglich eine valide Bitcoin-Adresse benötigt, nach der Anmeldung kann der Nutzer dann die Parameter (z.B. Höhe des Lösegelds angeben) und erhält eine Übersicht, wie viele Systeme bereits infiziert sind. Der Trojaner ist mit dem Frameworks NW.js entwickelt, welches bei Entwicklern durchaus einen populären und vertrauenswürdigen Status genießt. Dementsprechend sind mit dem Framework entwickelte Applikationen auch bei Anti-Viren Produkten oft als vertrauenswürdig eingestuft, sodass im Fall von Ransom32 die Erkennung sehr schlecht ausgefallen ist. Lediglich 3 von 54 Herstellern stuften die Malware als gefährlich ein.[3]
Bewertung:	Die Programmierung in JavaScript ermöglicht eine hohe Portierbarkeit auf diverse Betriebssysteme, da JavaScript plattformübergreifend eingesetzt werden kann. Die Entwickler müssen dabei lediglich die Pfade, in denen der Trojaner Verschlüsselungs-Operationen durchführen soll, auf die unterschiedlichen Betriebssysteme anpassen. Da Desktop-Applikationen, die in JavaScript geschrieben sind, nicht durch klassisches Sandboxing wie beispielsweise ausgeführtes JavaScript im Browser geschützt sind, können mitunter tiefe Einschnitte im System vorgenommen werden, wobei Krypto-Trojaner primär auf die Verschlüsselung persönlicher Dateien und nicht auf System-Dateien ausgelegt sind.
Empfehlung:	Die Empfehlungen zum Schutz vor Krypto-Trojanern bleiben unverändert. Die Entwicklung (sofern noch nicht geschehen) einer detaillierten Datensicherungs-Strategie sollte nach wie oberste Priorität haben. Eine grundlegende Sensibilisierung der Mitarbeiter (Umgang mit E-Mails und unbekannten Dateien) kann hier ebenfalls potenziellen Schäden vorbeugen.
Quellen:	[1] Meet Ransom32: The first JavaScript ransomware [2] vgl. CSCC-Lagebericht vom 29. Mai 2015 [3] https://www.virustotal.com, Stand 31. Dezember 2015
Point of Contact:	André Zingsheim, andre.zingsheim@it-tuv.com, 0221/969789-82

2016-01: Support-Ende für ältere Versionen des Internet Explorer

Titel **Support-Ende für ältere Versionen des Internet Explorer**	Risiko ■■■■■
Betroffene Systeme:	Internet Explorer < 11
Sachstand:	Microsoft stellt ab dem 12. Januar 2016 den Support für ältere Versionen (< 11) des Internet Explorers ein. Da ab diesem Zeitpunkt keine Sicherheitsupdates mehr zur Verfügung gestellt werden, stellt der Einsatz von älteren Versionen des Browsers ein hohes Sicherheitsrisiko dar. Für Applikationen, die nicht mit dem Internet Explorer 11 kompatibel sind, bietet Microsoft den Unternehmensmodus[2] des Browsers an, in dem durch eine verbesserte Rückwärtskompatibilität auch Applikationen lauffähig sein sollen, die primär für ältere Versionen des Browsers entwickelt worden sind.
Bewertung:	Der Internet Explorer war bisher immer ein beliebtes Ziel unter Angreifern, da Unternehmen insbesondere durch eigens entwickelte Applikationen, die nicht unter anderen Browsern lauffähig sind, an den Browser gebunden werden. Durch die zukünftig fehlende Bereitstellung von Sicherheitsupdates wird der Browser weiter in den Fokus von Angreifern rücken. Es ist davon auszugehen, dass nicht allen Unternehmen die rechtzeitige Migration auf die aktuelle Version gelingt, wodurch sich für Angreifer erhöhte Chancen auf eine erfolgreiche Kompromittierung bieten.
Empfehlung:	Aufgrund der hohen Attraktivität für Angreifer sollte der Internet Explorer auf keinen Fall in einer veralteten, nicht mit Sicherheitsupdates versorgten, Version betrieben werden. Sollten Applikationen nicht mit der aktuellen Version kompatibel sein, empfiehlt sich zuerst die Verwendung eines alternativen Browsers. Sofern auch dies nicht zu einer Lösung führt, müssen erweiterte, fortgeschrittene Sicherheitskonzepte entworfen werden.
Quellen:	[1] End of IE support [2] https://technet.microsoft.com/de-de/browser/dn508446
Point of Contact:	André Zingsheim, andre.zingsheim@it-tuv.com, 0221/969789-82

Informationsquellen

Für die Erstellung des wöchentlichen Lagebilds werden Informationen über Schwachstellen aus öffentlichen und nicht-öffentlichen Quellen gesammelt, konsolidiert und für die Gesamtlage aufbereitet. Genutzte Quellen sind unter anderem:

- NIST[2] National Vulnerability Database (https://nvd.nist.gov/Home/Email-List)
- Alerts/Bulletins des US-CERT (https://www.us-cert.gov/)
- CERT-Bund Advisories (https://www.cert-bund.de/)
- Security-Mails des RUS-CERT (http://cert.uni-stuttgart.de/)
- Hinweise des Bürger-CERT (https://www.buerger-cert.de/)
- Sicherheitsmeldungen der CSCC-Teilnehmer
- Erkenntnisse aus Penetrationstests und Sicherheitsanalysen der TÜV TRUST IT
- Sonstige öffentliche und nicht-öffentliche Quellen zur IT-Sicherheitslage

Die im Verlauf der Woche gemeldeten Sicherheitsinformationen werden in Top 2 der wöchentlichen Telefonkonferenz vorgestellt.

[2] National Institute of Standards and Technology