Bundesamt
für Sicherheit in der
Informationstechnik

Merkblatt zum sicheren Informationsaustausch mit dem Traffic Light Protocol (TLP), Version 2.0

Das Traffic Light Protocol (TLP) ist eine standardisierte Vereinbarung zum Austausch schutzwürdiger aber nicht formell eingestufter Informationen. Alle Dokumente werden in TLP-Stufen eingeteilt, die die Bedingungen für ihre Weitergabe regeln.

Das TLP regelt nicht den Schutz staatlich geheimzuhaltender Informationen. Dieser ist in der Verschlusssachenanweisung des Bundes[1] geregelt.

Die vom BSI verwendete TLP-Version 2.0 basiert auf der Definition der TLP Version 2.0[2] des „Forum of Incident Response and Security Teams“ (FIRST).

Im TLP-Informationsaustausch können folgende Rollen unterschieden werden:

- **Informationsersteller**
- **Verteiler** (z. B. BSI, CERT, SPOC, Verbände)
- **Empfänger** (z. B. Behörden, Betreiber, Unternehmen),
- ggf. **Partner** des Empfängers (i. d. R. vertraglich verbundene Organisationen, entweder als Dienstleister oder als Kunden)

Die Einschränkungen zur Weitergabe betreffen Verteiler, Empfänger und Partner.

Das TLP dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen durch Regelungen der Weitergabe. Eine unbefugte Weitergabe kann eine Verletzung der Vertraulichkeit, eine Rufschädigung, eine Beeinträchtigung der Geschäftstätigkeit oder datenschutzrechtlicher Belange zur Folge haben. **Im Zweifelsfall ist immer in Absprache mit dem Informationsersteller zu handeln.**

Durch die Unterschrift auf der TLP-Verpflichtung erklären natürliche und juristische Personen ihre Verpflichtung, die Regeln des TLP einzuhalten. Diese Verpflichtung endet nicht mit ihrer Zugehörigkeit zu einer bestimmten am TLP-basierten Informationsaustausch teilnehmenden Organisation. Eine Verpflichtung stellvertretend für den eigenen Verantwortungs- oder Zuständigkeitsbereich ist möglich. Werden Funktionspostfächer oder Gruppenrufnummern der Organisation angegeben, sind alle potenziellen Empfänger durch den Unterzeichner auf die Einhaltung des TLP zu belehren.

[1] Verschlusssachenanweisung, www.bsi.bund.de/dok/6602050
[2] Traffic Light Protocol – FIRST Standards Definitions and Usage Guidance 2.0, www.first.org/tlp

Die TLP-Stufen

TLP:CLEAR **Unbegrenzte Weitergabe**

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

Hinweis: TLP:CLEAR entspricht der Kennzeichnung TLP:WHITE der früheren Version 1.0 des TLP.

TLP:GREEN **Organisationsübergreifende Weitergabe**

Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe, wie beispielsweise Angehörige der Cybersecurity-Community, angehören.

TLP:AMBER **Eingeschränkte interne und organisationsübergreifende Weitergabe**

Der Empfänger darf die Informationen, welche als TLP:AMBER gekennzeichnet sind, an seine Partner weitergeben, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen. Eine Weitergabe von den Partnern an Dritte ist nicht erlaubt und sowohl in der eigenen Organisation als auch innerhalb der Partnerorganisation gilt das Prinzip „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen, diese müssen eingehalten werden.

TLP:AMBER+STRICT **Eingeschränkte interne Weitergabe**

Die Einstufung von Informationen als TLP:AMBER+STRICT beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers, jegliche Weitergabe darüber hinaus ist untersagt. Es gilt „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen, diese müssen eingehalten werden.

TLP:RED **Persönlich, nur für bekannte Empfänger**

Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden.

Allgemeine Hinweise

In diesem Dokument werden die Worte „muss“ und „sollte“ wie in RFC-2119[3] definiert verwendet.

Die Einstufung einer mündlichen Information wird vom Urheber vorgenommen und dem Zuhörerkreis stets vor der Weitergabe mitgeteilt. Personen, die nicht auf das TLP verpflichtet sind, müssen eine Besprechung für die Dauer der Weitergabe von als TLP:RED, TLP:AMBER, TLP:AMBER+STRICT und TLP:GREEN eingestuften Informationen verlassen.

Schriftstücke, die nach TLP eingestuft werden sollen, sind vom Informationsersteller vor Beginn des eigentlichen Informationsinhaltes auf jeder Seite des Dokuments mit dem Stichwort TLP:RED, TLP:AMBER,TLP:AMBER+STRICT, TLP:GREEN oder TLP:CLEAR deutlich zu kennzeichnen und nur berechtigten Personen auszuhändigen.

Bei jeder Weiterleitung muss gewährleistet werden, dass die weiteren Empfänger das TLP kennen und die damit verbundenen Regeln einhalten.

Elektronische Übertragung

Informationen der TLP-Stufen TLP:RED, TLP:AMBER und TLP:AMBER+STRICT müssen bei elektronischer Übertragung über ungeschützte Übertragungswege angemessen verschlüsselt werden.

Einstufung und Kennzeichnung

Einstufungen sind klar zu kennzeichnen. Sie gelten in der Regel auch für Auszüge aus eingestuften Dokumenten oder Informationen. Zusätzliche Einschränkungen für den Verteilerkreis können durch den Informationsersteller ergänzend zur TLP-Stufe eingebracht werden.

Werden mehrere Informationen unterschiedlicher TLP-Stufen zusammen gehandhabt, so sind sie entsprechend der höchsten vorliegenden TLP-Stufe zu behandeln.

Bei **Nachrichten** müssen Kennzeichnungen so erfolgen, dass sie für den Leser sofort deutlich erkennbar werden. Das TLP-Kennzeichen muss direkt vor der Information vorangestellt werden.

Bei **E-Mails** sollte das TLP-Kennzeichen zusätzlich vorangestellt im Betreff der E-Mail stehen.

Bei **Dokumenten** muss die Kennzeichnung in einer gut lesbaren Schriftgröße (12 pt oder größer) in der Kopf- und Fußzeile jeder Seite erfolgen. Bei der Schriftfarbe und dem Hintergrund für die Kennzeichen TLP:RED, TLP:AMBER, TLP:AMBER+STRICT, TLP:GREEN und TLP:CLEAR sollten die Vorgaben des „Traffic Light Protocol (TLP) – FIRST Standards Definitions and Usage Guidance – Version 2.0, Kapitel 2d“ eingehalten werden.

Bei **Dateien** sollte das TLP-Kennzeichen dem Dateinamen hinzuzugefügt werden.

[3] RFC 2119, https://www.rfc-editor.org/rfc/rfc2119 (muss=obligatorisch; sollte=wird empfohlen, falls nicht die spezifischen Umstände eine abweichende Vorgehensweise erfordern)

Weitergabe an nicht genehmigten Empfängerkreis

Sollte eine Weitergabe an einen durch die Einstufung nicht genehmigten Empfängerkreis notwendig werden, so ist diese vor der eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete in Zukunft nur noch Informationen der Stufe TLP:CLEAR.

Gekennzeichnete Dokumente (außer TLP:CLEAR) dürfen weder manuell noch automatisiert auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort Dritten zugänglich werden können.

Vervielfältigung

Die Vervielfältigung von TLP:AMBER, TLP:AMBER+STRICT und TLP:RED-Informationen muss auf das unbedingt notwendige Maß beschränkt werden. Vervielfältigungen sind genauso zu behandeln wie Originaldokumente einschließlich ihrer Kennzeichnung, Aufbewahrung, Weitergabe und Vernichtung.

Aufbewahrung

Informationen der TLP-Stufe TLP:AMBER, TLP:AMBER+STRICT und TLP:RED sollten auf mobilen Endgeräten verschlüsselt aufbewahrt werden. Papierdokumente der TLP-Stufen TLP:AMBER oder TLP:RED müssen in einem verschlossenen Behältnis aufbewahrt werden.

Vernichtung, Löschung und Aussonderung

Datenträger, auf denen Informationen der TLP-Stufen TLP:AMBER, TLP:AMBER+STRICT oder TLP:RED gespeichert wurden, müssen vor Aussonderung sicher gelöscht oder irreversibel physisch vernichtet werden. Papierdokumente der TLP-Stufen TLP:AMBER, TLP:AMBER+STRICT oder TLP:RED müssen in geeigneten Aktenvernichtern vernichtet werden.

Kompromittierung von Informationen

Bereits beim Verdacht auf Kompromittierung von Informationen (z. B. Versand an unberechtigte Dritte, Datenleaks, Upload auf externen Portalen wie Virustotal ...) sind umgehend der Informationsersteller und die für Sie zuständige Kontaktstelle des BSI (Nationales IT-Lagezentrum, CERT-Bund, KRITIS-Büro, etc.) zwecks Schadensminimierung über den Sachverhalt zu informieren.