# Responsible Disclosure Policy

## CERT NRW

Das Computer Emergency Response Team NRW ist zentrale Anlaufstelle der Landesverwaltung Nordrhein-Westfalens für präventive und reaktive Maßnahmen in Bezug auf sicherheits- und verfügbarkeitsrelevante Vorfälle in IT-Systemen.
Es dient als Informationsschnittstelle zwischen den Behörden und Einrichtungen der Landesverwaltung, dem technischen Know-How des Landesbetriebs IT.NRW (IT-Dienstleister der Landesverwaltung NRW) sowie anderen deutschen CERTs, insbesondere des Bundes und der Länder sowie in Unternehmen.

Sofern es der Schadensvermeidung dient, teilt das CERT NRW Informationen und Erkenntnisse über Schwachstellen in Hardware- und Software sowie Bedrohungen mit Kooperationspartnern wie dem Deutschen CERT-Verbund, dem VerwaltungsCERT-Verbund (VCV) und der Öffentlichkeit.

## Grundsätze

Für die verantwortungsvolle Weitergabe bzw. Veröffentlichung (Responsible Disclosure) hält sich das CERT NRW an folgende Grundsätze:

1. **Schadensvermeidung**
   Die Information potentieller Nutzer zwecks Schadensprävention hat Vorrang.

2. **Fairness**
   In sorgfältiger Abwägung unter Beachtung des ersten Grundsatzes berücksichtigen wir auch die Interessen der Hersteller betroffener Produkte.
   Die Umstände entscheiden über Art, Zeitpunkt und Empfängerkreis der Informationsweitergabe.

3. **Transparenz**
   Durch Veröffentlichung dieser Grundsätze legt das CERT NRW offen, wie und unter welchen Umständen Informationen weitergegeben oder veröffentlicht werden.
   Das CERT NRW wünscht sich eine positive Zusammenarbeit und Koordination mit betroffenen Herstellern und wird seine weitere Vorgehensweise stets klar kommunizieren.

Die Grundsätze 2. und 3. setzen voraus, dass die betroffenen Hersteller ebenfalls zu einer positiven Zusammenarbeit bereit sind und nach Kontaktaufnahme zeitnah und unbürokratisch mit dem CERT NRW in einen konstruktiven Dialog treten und selbst klar kommunizieren, welche Schritte zur Fehlerbehebung in welchem Zeitraum durch den Hersteller erfolgen werden.

# Bewertung und Umgang mit Schwachstelleninformationen

Laut obigem zweiten Grundsatz entscheiden die Umstände über Art, Zeitpunkt und Empfängerkreis der Informationsweitergabe.

Die Umstände ergeben sich unter anderem daraus, wie leicht und auf welchem Weg die Schwachstelle für Angriffe gegen IT-Systeme ausnutzbar ist, welche direkten und indirekten Folgen eine Ausnutzung der Schwachstelle hat bzw. haben kann, wie weit verbreitet das betroffene Produkt ist, um welche Art Systeme es sich handelt (z. B. kritische Infrastrukturen), ob bereits Angriffe auf die Schwachstelle stattgefunden haben und ob Exploits für die Schwachstelle oder Informationen zur Schwachstelle öffentlich oder in bestimmten Kreisen kursieren.

## *CVSS Scores*

Das CERT NRW nutzt zur Charakterisierung und Priorisierung von Schwachstellen das Common Vulnerability Scoring System[1], welches einige der oben genannten Einflussgrößen einbezieht.

## *Stufen der Vertraulichkeit*

Die Behandlung und Weitergabe von Schwachstelleninformationen unter Kooperationspartnern des CERT NRW erfolgt in der Regel auf Basis des Traffic Light Protocol[2].

Für die Einstufung von Schwachstelleninformationen nach TLP durch das CERT NRW gelten folgende Kriterien:

- TLP-RED bei besonders kritischen Schwachstellen, gegen deren Ausnutzung es aktuell keinen Schutz gibt, die kritische Infrastrukturen betreffen, leicht auszunutzen sind und deren vorzeitiges öffentliches Bekanntwerden zu Schäden großen Ausmaßes führen kann
- TLP-AMBER, für alle Fälle, in denen noch keine Fehlerbehebung (Patch) oder behelfsmäßige Schutzmaßnahme (Workaround) verfügbar ist
- TLP-GREEN oder TLP-WHITE in allen anderen Fällen

Die Behandlung von als Verschlusssache klassifizierten Informationen unterliegt den Bestimmungen des Geheimschutzes und wird hier nicht ausgeführt.

[1] http://nvd.nist.gov/cvss.cfm?calculator&version=2
[2] http://de.wikipedia.org/wiki/Traffic_Light_Protocol

## *Gültigkeitsdauer der TLP-Einstufung*

Schwachstelleninformationen, die TLP-AMBER eingestuft sind, werden nach Verfügbarkeit einer Fehlerbehebung automatisch auf TLP-WHITE herabgestuft.

45 Tage nach Kontaktaufnahme zum Hersteller werden die Informationen automatisch von TLP-AMBER auf TLP-GREEN herabgestuft, auch wenn der Hersteller bis dahin keine Fehlerbehebung zur Verfügung gestellt hat.[3]

Alle nach TLP eingestuften Schwachstelleninformationen werden spätestens ein Jahr nach Kontaktaufnahme zum Hersteller automatisch auf TLP-WHITE herabgestuft, außer es liegen zwingende Gründe vor, die dagegen sprechen.

Die Gründe müssen dem CERT NRW unaufgefordert in schriftlicher Form vorgelegt werden. Das CERT NRW entscheidet dann nach eingehender Prüfung und Abwägung über die weitere vorläufige TLP-Einstufung.

## *Weitergabe und Veröffentlichung*

Das CERT NRW tauscht unter Vertraulichkeitsvereinbarungen und Nutzung des TLP sicherheitsrelevante Informationen mit Computer Emergency Response Teams aus Industrie und Verwaltung.

Eine unverzügliche Weitergabe von Schwachstelleninformationen erfolgt parallel zur Kontaktaufnahme mit dem Hersteller, wenn eine oder mehrere der folgenden Bedingungen erfüllt sind:

- die Schwachstelle hat einen CVSS Base Score >= 7
- die Schwachstelle wird/wurde aktiv ausgenutzt

Die Weitergabe erfolgt in diesen Fällen in der Regel auf Need-To-Know-Basis (TLP-AMBER) oder TLP-RED, sofern keine Einstufung nach Verschlusssachenanweisung (VSA) vorliegt.

In allen anderen Fällen werden Schwachstelleninformationen 30 Tage nach Benachrichtigung des Herstellers durch das CERT NRW an die Kooperationspartner weiter gegeben.

Alle durch das CERT NRW nach TLP-WHITE eingestuften Schwachstelleninformationen werden durch das CERT NRW der Öffentlichkeit zur Verfügung gestellt, sofern eine Veröffentlichung dem ersten Grundsatz (Schadensvermeidung) dient und betroffenen Nutzern die Möglichkeit gibt, sich zu schützen.

Das CERT NRW veröffentlicht keinen Exploit Code sondern nur solche Informationen, die der Warnung und Prävention dienen.

[3] Zum Vergleich: das CERT Coordination Center (CERT CC) veröffentlicht alle Schwachstelleninformationen 45 Tage nach Kontaktaufnahme zum Hersteller, unabhängig von der Verfügbarkeit eines Patches oder Workarounds, siehe http://www.cert.org/kb/vul_disclosure.html

## Kontaktaufnahme mit Herstellern

Sobald das CERT NRW Kenntnis von einer Schwachstelle erlangt, sucht das CERT NRW schnellstmöglich Kontakt zu den betroffenen Herstellern, um diese über die Schwachstelle zu informieren.

Das CERT NRW kontaktiert zunächst die bekannten Ansprechpartner des CERTs des Herstellers, sofern diese bekannt sind.

Andernfalls, versucht das CERT NRW die entsprechenden Kontaktdaten über die Webseite des Herstellers zu ermitteln. Dabei ist es sehr hilfreich, wenn der Hersteller auf seiner Webseite Kontaktdaten für das Einsenden sicherheitsrelevanter Informationen an prominenter, leicht aufzufindender Stelle hinterlegt.

Der BSI-Veröffentlichung zur Cyber-Sicherheit „Handhabung von Schwachstellen[4]“ können Hersteller Empfehlungen zur Gestaltung des Prozesses zum Umgang mit Schwachstellen entnehmen.

Das CERT NRW informiert betroffene Hersteller über die erste Einstufung, Weitergabe und Veröffentlichung von Schwachstelleninformationen.

Es stellt dem Hersteller alle vorliegenden Informationen zur Schwachstelle zur Verfügung und steht dem Hersteller gerne für Rückfragen zur Verfügung.

Das CERT NRW bemüht sich unter Berücksichtigung der drei Grundsätze Schadensvermeidung, Fairness und Transparenz, die Interessen des Herstellers bestmöglich zu berücksichtigen.

Bei entsprechender Kooperationsbereitschaft und Transparenz auf Seiten des Herstellers und bei plausibler Begründung ist das CERT NRW unter Abwägung der Risiken für die betroffenen Anwender bereit, eine anstehende Veröffentlichung oder TLP-Herabstufung um bis zu drei Monate zu verschieben.

Kein Aufschub gewährt wird in folgenden Fällen:

- es sind Angriffe oder Software im Umlauf, welche die Schwachstelle ausnutzen
- die Schwachstelle ist leicht ausnutzbar (z. B. durch Eintippen einer URL im Browser)
- die Schwachstelle ist stark exponiert, weit verbreitet und für Angreifer leicht zu finden

[4] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/programmierung/BSI-CS_019.pdf?__blob=publicationFile