Lücken schließen. 

Der verantwortungsbewusste Umgang mit IT-Sicherheitslücken

Dr. Oliver Vettermann
– FIZ Karlsruhe, Leibniz-Institut für Informationsinfrastruktur

Status quo: unsichere IT-Sicherheitsforschung

Offenlegung von Softwarelücken: Rechtsstreit endet mit Vergleich

Forscher mit der Urheberrechtskeule an der Veröffentlichung von Softwarelücken zu hindern, widerspreche gesundem Menschenverstand, befand ein Landgericht.

Lesezeit: **4 Min.** 126

Dritte Zivilkammer des Landgerichts Nürnberg-Fürth unter dem Vorsitz von Ulrich Dettenhofer
(Bild: heise online/Ermert)

06.09.2018 12:36 Uhr

Von Monika Ermert

heise-Meldung vom 6.9.2018

Modern Solution: Staatsanwaltschaft scheitert mit Anklage gegen IT-Experten

Ein Programmierer deckte 2021 eine grobe Sicherheitslücke in der Software des deutschen E-Commerce-Unternehmens auf und wurde dafür angezeigt.

Lesezeit: **6 Min.** 128

(Bild: Wirestock Images/Shutterstock.com)

09.06.2023 17:15 Uhr

Von Fabian A. Scherschel

heise-Meldung vom 9.6.2023

Status quo: unsichere IT-Sicherheitsforschung

Koalitionsvertrag 2021-2025 🔗

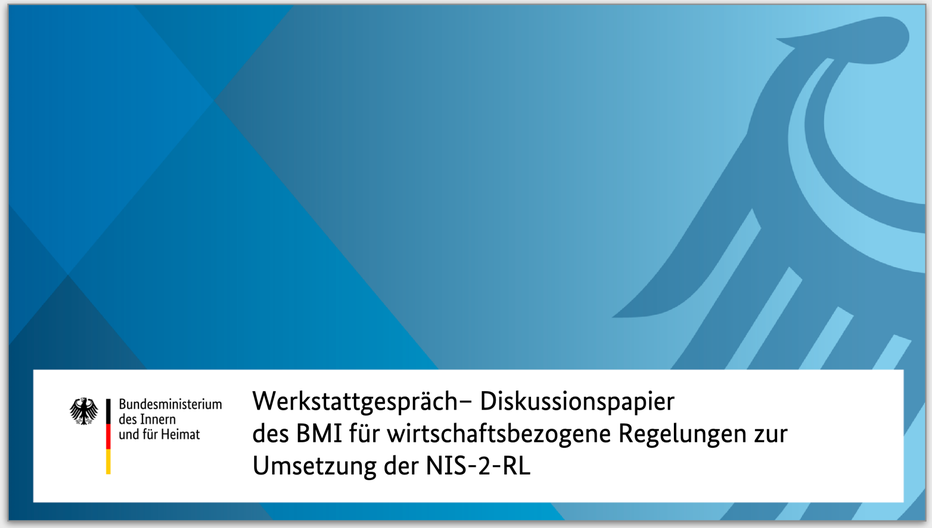
Digitale Bürgerrechte und IT-Sicherheit

Wir stärken digitale Bürgerrechte und IT-Sicherheit. Sie zu gewährleisten ist staatliche Pflicht. Wir führen ein Recht auf Verschlüsselung, ein wirksames Schwachstellenmanagement, mit dem Ziel Sicherheitslücken zu schließen, und die Vorgaben „security-by-design/default“ ein. Auch der Staat muss verpflichtend die Möglichkeit echter verschlüsselter Kommunikation anbieten. Hersteller haften für Schäden, die fahrlässig durch IT-Sicherheitslücken in ihren Produkten verursacht werden. Die Cybersicherheitsstrategie und das IT-Sicherheitsrecht werden weiterentwickelt. Darüber hinaus sichern wir die digitale Souveränität, u. a. durch das Recht auf Interoperabilität und Portabilität sowie das Setzen auf offene Standards, Open Source und europäische Ökosysteme, etwa bei 5G oder KI. Wir leiten einen strukturellen Umbau der IT-Sicherheitsarchitektur ein, stellen das Bundesamt für Sicherheit in der Informationstechnik (BSI) unabhängiger auf und bauen es als zentrale Stelle im Bereich IT-Sicherheit aus. Wir verpflichten alle staatlichen Stellen, ihnen bekannte Sicherheitslücken beim BSI zu melden und sich regelmäßig einer externen Überprüfung ihrer IT-Systeme zu unterziehen. Das Identifizieren, Melden und Schließen von Sicherheitslücken in einem verantwortlichen Verfahren, z. B. in der IT-Sicherheitsforschung, soll legal durchführbar sein. Hackbacks lehnen wir als Mittel der

16

Cyberabwehr grundsätzlich ab. Nicht-vertrauenswürdige Unternehmen werden beim Ausbau kritischer Infrastrukturen nicht beteiligt.

Status quo: unsichere IT-Sicherheitsforschung



Zusammenfassung des Diskussionspapiers auf Blog
von Prof. Dennis-Kenji Kipker, 31.10.2023 🔗

Lagebild der IT-Sicherheit in Deutschland,
2.11.2023 🔗

Verantwortungsvoller Umgang mit Sicherheitslücken

1. **Schaffen eines Rechtsrahmens in allen betroffenen Disziplinen**
   - Abbau strafrechtlicher Hürden – „Hackerparagraph“ und § 202a Abs. 1 StGB, z.B. durch spezielle Ausnahmeregelung für IT-Sicherheitsforschende
   - Abbau zivil- und urheberrechtlicher Möglichkeiten, Schranken als Hindernis für Wissenschaft und Forschung zu nutzen
   - Hinwirken auf einen klaren und verständlichen Rechtsrahmen sowie Begriffsklärung zum Abbau von Hürden (Stichwort: Dekompilieren)
2. **Etablieren einer Melde- und Koordinierungsstelle**
   - vertrauenswürdige, unabhängige Stelle – frei von politischen Interessen
   - verschiedene Melde-Modelle: von offen + bidirektional bis anonym und einmalig
   - Unterstützung von Anreizmechanismen (z.B. Bug Bounty der Hersteller)

Ausblick: NIS-2-Richtlinie und Cyber Resilience Act

Artikel 12

Koordinierte Offenlegung von Schwachstellen und eine europäische Schwachstellendatenbank

(1) Jeder Mitgliedstaat benennt eines seiner CSIRTs als Koordinator für die Zwecke einer koordinierten Offenlegung von Schwachstellen. Das als Koordinator benannte CSIRT fungiert als vertrauenswürdiger Vermittler und erleichtert erforderlichenfalls die Interaktion zwischen der eine Schwachstelle meldenden natürlichen oder juristischen Person und dem Hersteller oder Anbieter der potenziell gefährdeten IKT-Produkte oder IKT-Dienste auf Ersuchen einer der beiden Seiten. Zu den Aufgaben des als Koordinator benannten CSIRT gehört insbesondere

a) betreffende Einrichtungen zu ermitteln und zu kontaktieren,

b) die natürlichen oder juristischen Personen, die eine Schwachstelle melden, zu unterstützen, und

c) Zeitpläne für die Offenlegung auszuhandeln und das Vorgehen bei Schwachstellen zu koordinieren, die mehrere Einrichtungen betreffen.

Die Mitgliedstaaten stellen sicher, dass natürliche oder juristische Personen dem als Koordinator benannten CSIRT eine Schwachstelle, auf Wunsch anonym, melden können. Das als Koordinator benannte CSIRT stellt sicher, dass in Bezug auf die gemeldete Schwachstelle sorgfältige Folgemaßnahmen durchgeführt werden, und sorgen für die Anonymität der die Schwachstelle meldenden natürlichen oder juristischen Person. Wenn die gemeldete Schwachstelle erhebliche Auswirkungen auf Einrichtungen in mehreren Mitgliedstaaten haben könnte, arbeitet das als Koordinator benannte CSIRT jedes betreffenden Mitgliedstaats gegebenenfalls mit den anderen als Koordinatoren benannten CSIRTs innerhalb des CSIRTs-Netzwerks zusammen.

NIS-2-Richtlinie 🔗

2. ANFORDERUNGEN AN DIE BEHANDLUNG VON SCHWACHSTELLEN

Die Hersteller der Produkte mit digitalen Elementen müssen

(1) Schwachstellen und Komponenten des Produkts ermitteln und dokumentieren, u. a. durch Erstellung einer Software-Stückliste in einem gängigen maschinenlesbaren Format, aus der zumindest die obersten Abhängigkeiten des Produkts hervorgehen;

(2) im Hinblick auf die Risiken im Zusammenhang mit den Produkten mit digitalen Elementen unverzüglich Schwachstellen behandeln und beheben, unter anderem durch Bereitstellung von Sicherheitsaktualisierungen;

(3) die Sicherheit des Produkts mit digitalen Elementen regelmäßig und wirksam testen und überprüfen;

(4) sobald eine Sicherheitsaktualisierung bereitgestellt worden ist, Informationen über beseitigte Schwachstellen veröffentlichen, einschließlich einer Beschreibung der Schwachstellen mit Angaben, anhand deren die Nutzer das betroffene Produkt mit digitalen Elementen, die Auswirkungen der Schwachstellen und ihre Schwere erkennen können, sowie Informationen, die den Nutzern helfen, die Schwachstellen zu beheben;

(5) eine Strategie für die koordinierte Offenlegung von Schwachstellen aufstellen und umsetzen;

(6) Maßnahmen ergreifen, um den Austausch von Informationen über mögliche Schwachstellen in ihrem Produkt mit digitalen Elementen und darin enthaltenen Komponenten Dritter zu erleichtern, und dazu u. a. eine Kontaktadresse für die Meldung der in dem Produkt mit digitalen Elementen entdeckten Schwachstellen angeben;

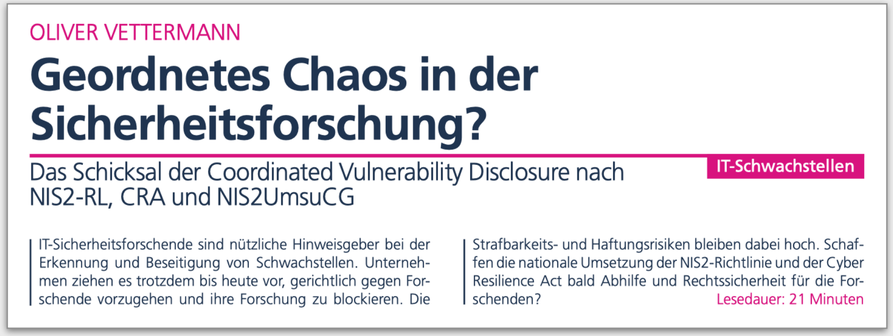
(7) Mechanismen für die sichere Verbreitung von Aktualisierungen für Produkte mit digitalen Elementen bereitstellen, damit ausnutzbare Schwachstellen rechtzeitig behoben oder eingedämmt werden;

(8) dafür sorgen, dass Sicherheits-Patches oder -Aktualisierungen, die zur Bewältigung festgestellter Sicherheitsprobleme zur Verfügung stehen, unverzüglich und kostenlos verbreitet werden, zusammen mit Hinweisen und einschlägigen Informationen, auch über zu treffende mögliche Maßnahmen.

Cyber Resilience Act – Anhang I Abschn. 2, Entwurf v. 15.9.2022 🔗

Vielen Dank für Ihre und Eure Aufmerksamkeit!

zum bidt Impuls:



erscheint in der Ausgabe 11/2023 der Multimedia & Recht (MMR) 🔗