security.txt

Dezernat 4

Bürgerservice, öffentliche Ordnung, Personal und IT

stadt oberhausen

security.txt

Vom **Umgang mit Schwachstellenmeldungen** und **Responsible Disclosure Prozessen** zur Etablierung einer Richtlinie zur **Meldung von Schwachstellen**.

Quellen:
"Computer Data Hacker" by Visual Content is licensed under CC BY 2.0.

Quellen:
"Computer Data Hacker" by Visual Content is licensed under CC BY 2.0.
"Das Telefonbuch. Was waren das für Zeiten als wir im Telefonbuch eine Nummer suchten." by guibro@ymail.com is licensed under CC BY-SA 2.0.
"Kurzer Dienstweg" by bebal is licensed under CC BY 2.0.

heise online > Security > WTF: Polizei rückte Samstagnacht wegen Zero-Day aus

WTF

WTF: Polizei rückte Samstagnacht wegen Zero-Day aus

Wegen der Sicherheitslücke in Windchill und ZeroPLM schickten mehrere Landeskriminalämter Polizeibeamte zu betroffenen Unternehmen. Die sind irritiert.

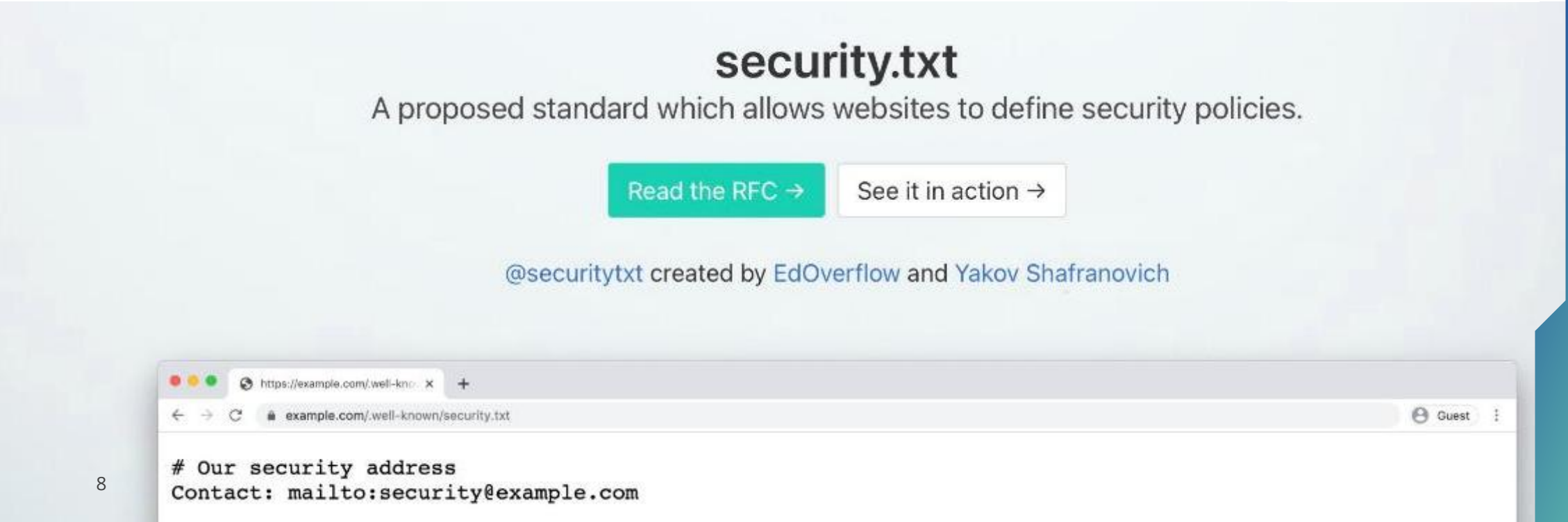
Quellen:
"Computer Data Hacker" by Visual Content is licensed under CC BY 2.0.
"Das Telefonbuch. Was waren das für Zeiten als wir im Telefonbuch eine Nummer suchten." by guibro@ymail.com is licensed under CC BY-SA 2.0.
"Kurzer Dienstweg" by bebal is licensed under CC BY 2.0.
Screenshot: heise.de; 24.03.2026

Wir brauchen einen Standard!

Wir brauchen einen Standard!

- RFC 9116: security.txt
- „Proposed Standard“; „Informational“
- Aber: anerkannt und weit verbreitet!

Quelle:
Screenshot securitytxt.org



Beispiel: securitytxt.org/.well-known/security.txt

Contact: https://hackerone.com/ed

Expires: 2026-03-27T00:00:00.000Z

Beispiel: securitytxt.org/.well-known/security.txt

Contact: https://hackerone.com/ed

Expires: 2026-03-27T00:00:00.000Z

Acknowledgments: https://hackerone.com/ed/thanks

Preferred-Languages: en, fr, de

Canonical: https://securitytxt.org/.well-known/security.txt

Policy: https://hackerone.com/ed?type=team&view_policy=true

Optional:

Danksagungen

Sprachen

Richtlinie

Verschlüsselung/GPG Key ID

Stellenangebote

Unsere Erfahrungen

security.txt wird genutzt

Initial wurden geringfügige Schwachstellen gemeldet

Meldungen häufig in gleicher Form und Struktur

Dann: Fragen nach Bug Bounties

Wir brauchen eine Richtlinie zur Meldung von Schwachstellen …

Bug Bounties …?

Prozess …?

„Hackerparagraph“ …?

Wir brauchen eine Richtlinie zur Meldung von Schwachstellen …

Bug Bounties …?

- Hall of Fame
- „Auf Vorschlag des Bereichs IT kann der Rat der Stadt Oberhausen eine darüber hinaus gehende Anerkennung aussprechen.“

Prozess …?

„Hackerparagraph“ …?

Wir brauchen eine Richtlinie zur Meldung von Schwachstellen …

Bug Bounties …?

- Hall of Fame
- „Auf Vorschlag des Bereichs IT kann der Rat der Stadt Oberhausen eine darüber hinaus gehende Anerkennung aussprechen.“

Prozess …?

- Responsible Disclosure statt Full Disclosure
- Öffentlichkeit erst nach Fix der Schwachstelle

„Hackerparagraph“ …?

Wir brauchen eine Richtlinie zur Meldung von Schwachstellen …

Bug Bounties …?

- Hall of Fame
- „Auf Vorschlag des Bereichs IT kann der Rat der Stadt Oberhausen eine darüber hinaus gehende Anerkennung aussprechen.“

Prozess …?

- Responsible Disclosure statt Full Disclosure
- Öffentlichkeit erst nach Fix der Schwachstelle

„Hackerparagraph“ …?

- „Sofern das Handeln von Sicherheitsforschenden den vorgenannten Vorgaben entspricht, erfolgt keine Einbindung von Strafverfolgungsbehörden. Dies gilt nicht, wenn erkennbar kriminelle Absichten verfolgt werden.“

Mögliche Probleme?

Lt. RFC ist eine separate security.txt pro Domain, Subdomain und IP notwendig!

Technisch

- Bereitstellung auf Appliances?
- Rewrite in Reverseproxy?
- Systeme ohne Webservice?

Organisatorisch

Aktualität auf allen Systemen sicherstellen?

Praktische Erfahrung

security.txt der Hauptdomain wird genutzt.

Mitmachen und nachnutzen!

- Prozess definieren
- Empfänger festlegen
- Empfangsbereitschaft sicherstellen
- security.txt publizieren
- Gegebenenfalls Richtlinie publizieren

Bei Fragen

Kontaktdaten

Stadt Oberhausen
Bereich 4-4 / IT
46042 Oberhausen

tobias.scherbaum@oberhausen.de

https://www.oberhausen.de
/.well-known/security.txt