# Von der Sicherheitslücke zum Fix: Wie Unternehmen mit Sicherheitslücken (nicht) umgehen sollten

## Security Transparent 2018

Sebastian Neef
IT Solutions Neef / Internetwache.org

8. Mai 2018

# Wer bin ich?

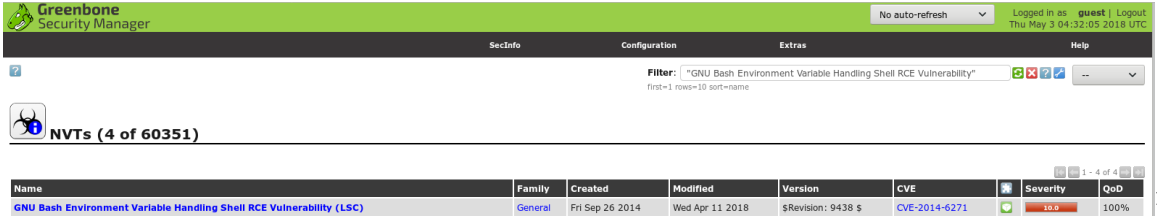
- Sebastian Neef (@gehaxelt)
- MSc Informatik an der TU Berlin
  - Fokus auf IT-Sicherheit
  - Internationale Hacking Wettbewerbe als ENOFLAG
- "Guter" Hacker
  - Security Research auf `0day.work` und `internetwache.org`
  - Systematische Scans des Internets
  - Aufdeckung von Sicherheitslücken und Angriffen
- Selbstständig
  - Freiberufler im IT-Securityfeld seit 2012
  - `it-solutions-neef.de`

# Was ist das Problem? (1)

## Sicherheitslücken!

1. Menschen machen Fehler.
2. Software und Hardware wird von Menschen entwickelt.
3. $\Rightarrow$ Software und Hardware hat Fehler!

# Was ist das Problem? (2)



[1]

The Heartbleed Bug

[2]

[3]

[1] Bild: secinfo.greenbone.net
[2] Bild: heartbleed.com
[3] Bild: Martin Wiesner

# Was ist das Problem? (3)

Wahrscheinlich wird aktuell irgendwo auf der Welt nach Sicherheitslücken gesucht und eine bisher unbekannte Schwachstelle entdeckt.

1. Sicherheitslücke finden
2. Proof of Concept / Exploit entwickeln
3. **???**
4. Profit! (?)

Was passiert bei Schritt 3?

# Was ist das Problem? (3)

Wahrscheinlich wird aktuell irgendwo auf der Welt nach Sicherheitslücken gesucht und eine bisher unbekannte Schwachstelle entdeckt.

1. Sicherheitslücke finden
2. Proof of Concept / Exploit entwickeln
3. **???**
4. Profit! (?)

Was passiert bei Schritt 3?

# Was passiert mit der Sicherheitslücke?

Je nach Charakter des "Hackers" gibt es verschiedene Optionen:

**"Blackhat"**

- Verkauf auf dem Schwarzmarkt
- (gezielte) Angriffe
- ⇒ Kein Patch erwünscht

**"Greyhat"**

- Full Disclosure
- Ggf. Nutzung von "Blackhats"
- ⇒ Eventuell ein Patch vom Hersteller

**"Whitehat"**

- Responsible Disclosure
- ⇒ Patch in Koordination mit dem Hersteller

# Wie mit Sicherheitslücken umgehen?

Sicherheitslücken auf [redacted]
› Sicherheitslücke auf [redacted]
Sicherheitslücken auf [redacted]
Sicherheitslücken auf [redacted]
› Sicherheitslücken auf [redacted].de
Sicherheitslücken auf [redacted].de
Sicherheitslücke auf [redacted]
Sicherheitslücken auf [redacted].de
Sicherheitslücken auf [redacted]de
Anfrage an Ansprechpartner : Sicherheitslücken
Sicherheitslücken auf [redacted]in.de
Fwd: AW: AW: Fragen zur Meldung von Sicherhe
Sicherheitslücke auf [redacted].de
› Sicherheitslücken auf [redacted]

- Wer von Ihnen hat eine gut auffindbare Kontaktmöglichkeit?
- Wer von Ihnen hat solche Hinweise bereits erhalten?

# Wie mit Sicherheitslücken umgehen?

Sicherheitslücken auf [redacted]
› Sicherheitslücke auf [redacted]
Sicherheitslücken auf [redacted]
Sicherheitslücken auf [redacted]
› Sicherheitslücken auf [redacted].de
Sicherheitslücken auf [redacted].de
Sicherheitslücke auf [redacted]
Sicherheitslücken auf [redacted].de
Sicherheitslücken auf [redacted]de
Anfrage an Ansprechpartner : Sicherheitslücken
Sicherheitslücken auf [redacted]in.de
Fwd: AW: AW: Fragen zur Meldung von Sicherhe
Sicherheitslücke auf [redacted].de
› Sicherheitslücken auf [redacted]

- Wer von Ihnen hat eine gut auffindbare Kontaktmöglichkeit?
- Wer von Ihnen hat solche Hinweise bereits erhalten?

# Wie mit Sicherheitslücken umgehen?

Sicherheitslücken auf [redacted]
› Sicherheitslücke auf [redacted]
Sicherheitslücken auf [redacted]
Sicherheitslücken auf [redacted]
› Sicherheitslücken auf [redacted].de
Sicherheitslücken auf [redacted].de
Sicherheitslücke auf [redacted]
Sicherheitslücken auf [redacted].de
Sicherheitslücken auf [redacted]de
Anfrage an Ansprechpartner : Sicherheitslücken
Sicherheitslücken auf [redacted]in.de
Fwd: AW: AW: Fragen zur Meldung von Sicherhe
Sicherheitslücke auf [redacted].de
› Sicherheitslücken auf [redacted]

- Wer von Ihnen hat eine gut auffindbare Kontaktmöglichkeit?
- Wer von Ihnen hat solche Hinweise bereits erhalten?

# Das Projekt Internetwache.org

Internetwache.org
Für ein sichereres Internet

- Gründung 2012 von Herrn Schäfers und meiner Wenigkeit
- Ethisches Hacken und Meldung von über +300 Sicherheitslücken
  - Wasserwerke, Ampel- und Windkraftanlagen, usw.
  - Phishing-Seiten, usw.
  - Paypal, Google, Facebook, usw.
- Systematische Internetscans
  - Scans der Alexa Top 1M
  - Untersuchung auf AXFR-Abfragen / .git-Ordner / .DS_Store-Dateien

# Positivbeispiel: Meldung einer XSS im OpenVAS/GSM (1)

## Kurzinfo CB-K16/0058

| 4 | Risiko: hoch |
|---|---|

### Information zu Schwachstellen und Sicherheitslücken

| | |
|---|---|
| Titel: | Greenbone Security Assistant: Eine Schwachstelle ermöglicht einen Cross-Site-Scripting-Angriff |
| Datum: | 13.01.2016 |
| Software: | Greenbone Security Assistant >= 6.0.0, Greenbone Security Assistant < 6.0.8, Greenbone OS >= 3.1.1, Greenbone OS <= 3.1.23 |
| Plattform: | GNU/Linux |
| Auswirkung: | Cross-Site-Scripting |
| Remoteangriff: | Ja, aus dem lokalen Netzwerk |
| Risiko: | hoch |
| Bezug: | Greenbone Security Advisory GBSA2016-01 |

# Positivbeispiel: Meldung einer XSS im OpenVAS/GSM (2)

## SECURITY RESPONSE TEAM

### So helfen wir Ihnen bei Sicherheitsproblemen in unseren Produkten

Bei auftauchenden **Sicherheitsproblemen** in unserem Produkt oder unserer Dienstleistung, bitte Nachricht an:

security@greenbone.net

E-Mail

Wir werden unmittelbar mit der Behebung der Sicherheitsprobleme beginnen und Sie über den Stand informiert halten.

# Positivbeispiel: Meldung einer XSS im OpenVAS/GSM (3)

- 07.01.2016, um 19:00: Untersuchung des OpenVAS und Entdeckung einer XSS
- 07.01.2016, um 22:38: Meldung der Lücke mit allen Details per verschlüsselter Email an security@greenbone.net
- 08.01.2016, um 11:01: Bestätigung der Lücke und Hinweis, dass seit 23:00 an einem Patch gearbeitet wird
- 08.01.2016, um 15:00: Follow-Up, dass Patch für OpenVAS bereit steht, aber weitere Tests durchgeführt werden.
- 09.01.2016: Neues Patch Level Release für GOS veröffentlicht
- 12/13.01.2016: OpenVAS Patches und Advisories veröffentlicht
- 18.01.2016: CVE-2016-1926 von der MITRE zugewiesen
- 20.01.2016: Blogpost auf internetwache.org veröffentlicht

# Positivbeispiel: Meldung einer XSS im OpenVAS/GSM (3)

- 07.01.2016, um 19:00: Untersuchung des OpenVAS und Entdeckung einer XSS
- 07.01.2016, um 22:38: Meldung der Lücke mit allen Details per verschlüsselter Email an security@greenbone.net
- 08.01.2016, um 11:01: Bestätigung der Lücke und Hinweis, dass seit 23:00 an einem Patch gearbeitet wird
- 08.01.2016, um 15:00: Follow-Up, dass Patch für OpenVAS bereit steht, aber weitere Tests durchgeführt werden.
- 09.01.2016: Neues Patch Level Release für GOS veröffentlicht
- 12/13.01.2016: OpenVAS Patches und Advisories veröffentlicht
- 18.01.2016: CVE-2016-1926 von der MITRE zugewiesen
- 20.01.2016: Blogpost auf internetwache.org veröffentlicht

# Positivbeispiel: Meldung einer XSS im OpenVAS/GSM (3)

- 07.01.2016, um 19:00: Untersuchung des OpenVAS und Entdeckung einer XSS
- 07.01.2016, um 22:38: Meldung der Lücke mit allen Details per verschlüsselter Email an security@greenbone.net
- 08.01.2016, um 11:01: Bestätigung der Lücke und Hinweis, dass seit 23:00 an einem Patch gearbeitet wird
- 08.01.2016, um 15:00: Follow-Up, dass Patch für OpenVAS bereit steht, aber weitere Tests durchgeführt werden.
- 09.01.2016: Neues Patch Level Release für GOS veröffentlicht
- 12/13.01.2016: OpenVAS Patches und Advisories veröffentlicht
- 18.01.2016: CVE-2016-1926 von der MITRE zugewiesen
- 20.01.2016: Blogpost auf internetwache.org veröffentlicht

# Positivbeispiel: Meldung einer XSS im OpenVAS/GSM (3)

- 07.01.2016, um 19:00: Untersuchung des OpenVAS und Entdeckung einer XSS
- 07.01.2016, um 22:38: Meldung der Lücke mit allen Details per verschlüsselter Email an security@greenbone.net
- 08.01.2016, um 11:01: Bestätigung der Lücke und Hinweis, dass seit 23:00 an einem Patch gearbeitet wird
- 08.01.2016, um 15:00: Follow-Up, dass Patch für OpenVAS bereit steht, aber weitere Tests durchgeführt werden.
- 09.01.2016: Neues Patch Level Release für GOS veröffentlicht
- 12/13.01.2016: OpenVAS Patches und Advisories veröffentlicht
- 18.01.2016: CVE-2016-1926 von der MITRE zugewiesen
- 20.01.2016: Blogpost auf internetwache.org veröffentlicht

# Positivbeispiel: Meldung einer XSS im OpenVAS/GSM (3)

- 07.01.2016, um 19:00: Untersuchung des OpenVAS und Entdeckung einer XSS
- 07.01.2016, um 22:38: Meldung der Lücke mit allen Details per verschlüsselter Email an security@greenbone.net
- 08.01.2016, um 11:01: Bestätigung der Lücke und Hinweis, dass seit 23:00 an einem Patch gearbeitet wird
- 08.01.2016, um 15:00: Follow-Up, dass Patch für OpenVAS bereit steht, aber weitere Tests durchgeführt werden.
- 09.01.2016: Neues Patch Level Release für GOS veröffentlicht
- 12/13.01.2016: OpenVAS Patches und Advisories veröffentlicht
- 18.01.2016: CVE-2016-1926 von der MITRE zugewiesen
- 20.01.2016: Blogpost auf internetwache.org veröffentlicht

# Positivbeispiel: Meldung einer XSS im OpenVAS/GSM (3)

- 07.01.2016, um 19:00: Untersuchung des OpenVAS und Entdeckung einer XSS
- 07.01.2016, um 22:38: Meldung der Lücke mit allen Details per verschlüsselter Email an security@greenbone.net
- 08.01.2016, um 11:01: Bestätigung der Lücke und Hinweis, dass seit 23:00 an einem Patch gearbeitet wird
- 08.01.2016, um 15:00: Follow-Up, dass Patch für OpenVAS bereit steht, aber weitere Tests durchgeführt werden.
- 09.01.2016: Neues Patch Level Release für GOS veröffentlicht
- 12/13.01.2016: OpenVAS Patches und Advisories veröffentlicht
- 18.01.2016: CVE-2016-1926 von der MITRE zugewiesen
- 20.01.2016: Blogpost auf internetwache.org veröffentlicht

# Positivbeispiel: Meldung einer XSS im OpenVAS/GSM (3)

- 07.01.2016, um 19:00: Untersuchung des OpenVAS und Entdeckung einer XSS
- 07.01.2016, um 22:38: Meldung der Lücke mit allen Details per verschlüsselter Email an security@greenbone.net
- 08.01.2016, um 11:01: Bestätigung der Lücke und Hinweis, dass seit 23:00 an einem Patch gearbeitet wird
- 08.01.2016, um 15:00: Follow-Up, dass Patch für OpenVAS bereit steht, aber weitere Tests durchgeführt werden.
- 09.01.2016: Neues Patch Level Release für GOS veröffentlicht
- 12/13.01.2016: OpenVAS Patches und Advisories veröffentlicht
- 18.01.2016: CVE-2016-1926 von der MITRE zugewiesen
- 20.01.2016: Blogpost auf internetwache.org veröffentlicht

# Positivbeispiel: Meldung einer XSS im OpenVAS/GSM (3)

- 07.01.2016, um 19:00: Untersuchung des OpenVAS und Entdeckung einer XSS
- 07.01.2016, um 22:38: Meldung der Lücke mit allen Details per verschlüsselter Email an security@greenbone.net
- 08.01.2016, um 11:01: Bestätigung der Lücke und Hinweis, dass seit 23:00 an einem Patch gearbeitet wird
- 08.01.2016, um 15:00: Follow-Up, dass Patch für OpenVAS bereit steht, aber weitere Tests durchgeführt werden.
- 09.01.2016: Neues Patch Level Release für GOS veröffentlicht
- 12/13.01.2016: OpenVAS Patches und Advisories veröffentlicht
- 18.01.2016: CVE-2016-1926 von der MITRE zugewiesen
- 20.01.2016: Blogpost auf internetwache.org veröffentlicht

# Positivbeispiel: Meldung einer XSS im OpenVAS/GSM (4)

| | | |
|---|---|---|
| Sicherheitslücke im Greenbone Security Manager | 07/01/16 22:38 | Internetwache PGP |
| Re: Sicherheitslücke im Greenbone Security Manager | 08/01/16 11:01 | Jan-Oliver Wagner |
| Re: Sicherheitslücke im Greenbone Security Manager | 08/01/16 11:23 | Internetwache PGP |
| Re: Sicherheitslücke im Greenbone Security Manag... | 08/01/16 15:18 | Jan-Oliver Wagner |
| Re: Sicherheitslücke im Greenbone Security Man... | 08/01/16 16:02 | Internetwache PGP |
| Re: Sicherheitslücke im Greenbone Security Man... | 08/01/16 16:32 | Jan-Oliver Wagner |
| Re: Sicherheitslücke im Greenbone Security ... | 08/01/16 16:40 | Internetwache PGP |
| Re: Sicherheitslücke im Greenbone Security ... | 08/01/16 17:36 | Jan-Oliver Wagner |

- Dediziertes security@ Postfach mit PGP-Schlüssel
- Sehr schnelle Reaktion!
- Freundliche und informative Kommunikation!
- Veröffentlichung eines Patches und Advisories!
  - `https://www.greenbone.net/security-response-team/`
  - `http://www.openvas.org/OVSA20160113.html`

# Negativbeispiele

- Keine oder nur schleppende Kommunikation oder Reaktion
  - Keine einfache Kontaktmöglichkeit (Supportformulare?)
  - Keine Möglichkeit, den richtigen Ansprechpartner zu sprechen.
- Leere Versprechungen oder kein Interesse das Problem zu beheben

  *Wir wissen leider nicht, wer für die Webseite zuständig ist.*

- Versuch, mögliche Veröffentlichung zu verbieten
- Versuch, rechtliche Schritte einzuleiten

  *Don't kill the messenger!*

- $\Rightarrow$ Gefährdung für das Unternehmen oder Kunden bleibt bestehen!

# Was sollte man jetzt tun?

- Einfache Kontaktmöglichkeit für Sicherheitslücken aufbauen und regelmäßig prüfen! (z.B.: Security.txt)
- Mit Sicherheitsforschern in enger Zusammenarbeit und Kommunikation verbleiben!
- Patches und Advisories veröffentlichen (inklusive CVE, falls möglich)!
- Beim Sicherheitsforscher für die aufgewendete Zeit bedanken!
- Security-Mailinglisten abonnieren und nach eigenen Produkten Ausschau halten.
- Responsible Disclosure oder BugBounty Programm starten!

# Schluss!

## Vielen Dank für Ihre Aufmerksamkeit!

- Es gibt immer etwas zu fragen oder diskutieren ! :=)
- Gern auch per Email an hallo@neef.it or im persönlichen Gespräch!

# Security Programme

- Grundidee: "Hack uns"
- Ausschreibung bestimmter Regeln
- Keine rechtlichen Schritte
- Plattformen: BugCrowd / HackerOne / SynAck

**Responsible Disclosure Programm**

- Eintragung in Hall of Fames
- Geschenke: Sticker, Tshirts, etc

**Bug Bounty Programm**

- Auszahlung je nach Schweregrad
- 50$ bis 40 000 $
- Zuschlag nur für Erstfinder

# Security.txt

- /.well-known/security.txt bzw. /security.txt
- Kontaktinformationen
  - Contact: [Email/Telefon/URL]
  - Encryption: Schlüssel für Verschlüsselung
  - Policy: [URL zur Security Policy]
  - Acknowledgments: [Liste mit Danksagungen]
- `https://securitytxt.org/` oder `https://tools.ietf.org/html/draft-foudil-securitytxt-03`