



**TASK FORCE**  
**IT - SICHERHEIT IN DER WIRTSCHAFT**  
Mehrwert und Schutz für Rechner.

Gefördert durch:



aufgrund eines Beschlusses  
des Deutschen Bundestages

# Initiative-S

## Der Webseiten-Check zur Sicherheit Ihres Internetauftritts



**INITIATIVE** **S**



**TASK FORCE**  
**IT - SICHERHEIT IN DER WIRTSCHAFT**  

---

**Mehrwert und Schutz für Rechner.**

Gefördert durch:

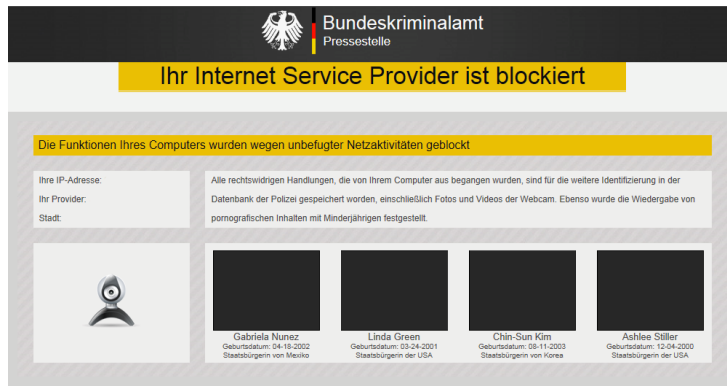


aufgrund eines Beschlusses  
des Deutschen Bundestages

## eco

Gründung:	1995/größter Internet-Verband in Europa
Vorstandsvorsitzender:	Prof. Michael Rotert
Mitgliedschaften:	INHOPE, EuroISPA, Euro-IX, FSM, RIPE
Kooperationen:	networker NRW e.V., TeleTrust, G.A.M.E.
Mitglieder:	aktuell mehr als 700 Mitglieder
Standorte:	Köln, Berlin, Hamburg, Frankfurt
DE-CIX:	mehr als 580 Kunden aus über 60 Ländern. Weltweit größter Datenaustauschknoten

# Risiko Schadprogramme



22.02.2013 13:59

« Vorige | Nächste »

## Zertifizierter Online-Banking-Trojaner

🔊 vorlesen / MP3-Download

Jean-Ian Boutin vom Antivirus-Hersteller Eset hat Trojaner entdeckt, die eine gültige digitale Signatur tragen. Damit schlüpfen die Online-Banking-Spione bei oberflächlichen Checks unter Umständen als harmlos durch. Das verwendete Code-Signing-Zertifikat hat offenbar der Zertifikatsherausgeber DigiCert ausgestellt – und zwar einer Firma, die es schon lang nicht mehr gibt.

Eine gültige Unterschrift der Firma "NS Autos" bestätigte deren Urheberschaft bei einer Reihe von Programmen, die sich [bei genauer Analyse](#) als Trojaner entpuppten – zumindest einige davon spezialisiert auf Online-Banking-Betrug. Eine Firma mit dem Namen NS Autos gab es zwar durchaus – allerdings wurde sie 2011 aufgelöst. Das hinderte den [Zertifikatsherausgeber DigiCert](#) offenbar nicht daran, ihr am 19. November 2012 ein gültiges Zertifikat für das Unterschreiben von ausführbaren Programmen auszustellen. Erst nach der Benachrichtigung durch Eset wurde das Zertifikat widerrufen.

- Vielfältige Infektionswege
- Ausnutzung von Sicherheitslücken in veralteter Software auf Systemen ohne entsprechende Schutzmechanismen (AV-Produkte)
- E-Mail-Anhänge oder Links
- Infizierte (vertrauenswürdige!) Webseiten
- Werbebanner
- Downloads
- USB-Sticks
- ...

## Was droht?

- Datendiebstahl (PIN, TAN, Login, Kreditkartendaten, Geschäftsgeheimnisse)
- Manipulation beim Online-Banking
- Spam-Versand
- Beteiligung bei DDoS-Angriffen
- Missbrauch von VoIP
- Missbrauch als Proxy

## Anti-Botnet Beratungszentrum

- Start in DE: 15.09.2010
- Hilft in 3 Schritten
  - Informieren / Säubern / Vorbeugen
- DE-Cleaner zum Download
- Anti-Bot CD
  - Neue Version seit Anfang September 2013
- Weitere Infos unter [blog.botfrei.de](http://blog.botfrei.de)
  - Mehr als 5 Millionen Besucher in 2012

botfrei



## Statistiken: Avira DE-Cleaner Logfile Analyse

gesendete Reports in 2012:

Anzahl Gescannter Systeme:	<b>213.812</b>
Summe nicht infizierter Systeme:	<b>142.778</b>
Summe infizierter Systeme:	<b>70.989</b>
	<b>(→ 33,20%)</b>

Durchschn. Anzahl infizierte Dateien/System: **7**

# Risiko infizierte Webseiten

22.02.2013 09:34

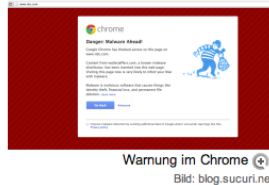
« Vorige | Nächste »

## Gehackte Website NBC.com infizierte Rechner

🔊 vorlesen / MP3-Download

Die Website des US-amerikanischen Fernsehsenders NBC ist gehackt worden und hat die Rechner von Besuchern mit Malware infiziert. Das hat eine Sprecherin des US-Konzern [gegenüber](#) der Huffington Post eingeräumt. [Laut](#) verschiedener Sicherheitsunternehmen hatten Hacker Zugriff auf die Server erlangt und bösartige IFrames in die Seiten eingebunden. Auf ungeschützten Computern sei darüber hinaus eine Variante des Bots Citadel installiert worden.

Wie lange die Gefahr bestanden hat, konnte die NBC-Sprecherin nicht sagen, sie habe aber versichert, dass die Website inzwischen wieder sauber ist: "Nutzer, die sie jetzt besuchen, sind sicher." Wie SurfRight schreibt, waren auch andere Seiten betroffen, beispielsweise die der Late-Night-Show von Jimmy Fallon. Laut einer [ausführlichen Erklärung](#) von SurfRight richteten sich die Angriffe gezielt gegen eine ältere Version von Adobes Acrobat Reader und Java.



## Sparkasse.de kurzzeitig von Hackerangriff betroffen

DSGV-Pressemitteilung - 19. Februar 2013

Die Sparkassen raten allen Internetnutzern, die gestern zwischen 12:45 Uhr und 17:05 Uhr auf den Internetseiten von Sparkasse.de waren, den eigenen Rechner mit einem gängigen, aktuellen Virenschutzprogramm zu durchsuchen.

Hintergrund ist ein Angriff Dritter auf die Seite von Sparkasse.de, bei dem eine Schadsoftware auf einzelnen Seiten von Sparkasse.de platziert werden konnte. Kunden, die ohne aktuellen und aktiven Virenschanner auf Sparkasse.de waren, könnten sich diese Schadsoftware auf den eigenen Rechner geladen haben. Sollte dies der Fall sein, kann die Schadsoftware mit allen gängigen Virenschutzprogrammen beseitigt werden.

- **Besuch einer Webseite allein reicht für eine Infektion aus**

- **80% aller Schadsoftware wird über giftige Webserver verteilt**

- **12% der Malware-verseuchten Webseiten stammen aus Deutschland (Quelle: Kaspersky)**

- **50% aller Webseitenbetreiber erfahren über eine Browserwarnung von der Infektion ihrer Seite (Quelle: Commtouch)**

# Was droht?



**Warnung: Irgendetwas stimmt hier nicht!**

**www.wetter.com** enthält Malware. Ihr Computer wird möglicherweise mit einem Virus infiziert, wenn Sie diese Website aufrufen.

Google hat schädliche Software gefunden, die möglicherweise auf Ihrem Computer installiert wird, wenn Sie fortfahren. Wenn Sie diese Website bereits in der Vergangenheit besucht haben oder dieser Website vertrauen, ist es möglich, dass sie vor Kurzem von einem Hacker manipuliert wurde. Sie sollten daher nicht fortfahren und den Vorgang vielleicht morgen wiederholen oder eine andere Website aufrufen.

Wir haben **www.wetter.com** bereits informiert, dass wir Malware auf der Website gefunden haben. Weitere Informationen zu den Problemen auf [www.wetter.com](http://www.wetter.com) erhalten Sie auf der [Google-SafeBrowsing-Diagnoseseite](#).

[Zurück](#)

Wenn Sie zur Kenntnis nehmen, dass diese Website Ihrem Computer schaden kann, [Trotzdem fortfahren](#).

Unterstützen Sie uns dabei, Malware zu erkennen, indem Sie uns zusätzliche Informationen zu Websites senden, auf denen diese Warnung erscheint. Diese Daten werden gemäß [Datenschutzbestimmungen von Safe Browsing](#) gehandhabt.

- Vertrauensverlust bei Kunden und Geschäftspartnern
- Infektion der eigenen Rechner
- Abschalten durch den Provider



## Vorbeugen. Untersuchen. Sicherheit genießen.

Schützen Sie Ihren Webauftritt und Ihre Besucher vor unbemerkten Manipulationen und erhalten Sie professionelle Hilfe.

Geben Sie hier den Namen Ihrer Internetadresse ein und registrieren Sie sich kostenlos.

**KOSTENFREI ANMELDEN****SEITENCHECK****SÄUBERN****SCHÜTZEN**

### Herzlich willkommen beim Seiten-Check der Initiative-S!

Mehr als die Hälfte aller Cyber-Angriffe weltweit betreffen nach Symantec's Internet Security Report bereits kleine und mittelständische Unternehmen. Mit Schadprogrammen infizierte Unternehmens-Webseiten sind im Internet eine Gefahr sowohl für Sie als Seitenbetreiber als auch für Ihre Kunden und Geschäftspartner.

Nutzen Sie den neuen Security-Service, den eco-Verband der deutschen Internetwirtschaft anbietet, um die IT-Sicherheit von Firmen und den Schutz im Internet zu erhöhen. Lassen Sie Ihren Internet-Auftritt einfach, bequem und kostenfrei von den Profis der Initiative-S online prüfen. Wie das funktioniert, erfahren Sie in den drei Schritten: Seitencheck, Säubern und Schützen.



Unternehmen, die die Sicherheit ihrer Webseiten regelmäßig prüfen lassen, können ihren Internetauftritt jetzt auch mit einem Sicherheits-Siegel versehen.



**TASK FORCE**  
**IT-SICHERHEIT IN DER WIRTSCHAFT**  
Mehrwert und Schutz für Rechner.



# TASK FORCE IT - SICHERHEIT IN DER WIRTSCHAFT

## Mehrwert und Schutz für Rechner.

Gefördert durch:



aufgrund eines Beschlusses  
des Deutschen Bundestages

INITIATIVE<sup>S</sup>

Eine Initiative von: Gefördert durch: aufgrund eines Beschlusses des Deutschen Bundestages

Startseite Schützen Säubern Über das Projekt Teilnehmer Kontakt

SEITENCHECK  
ALS MITGLIED PROFITIEREN

**Ihre Domain "eco.de" für das regelmäßige Monitoring durch die Initiative-S anmelden**

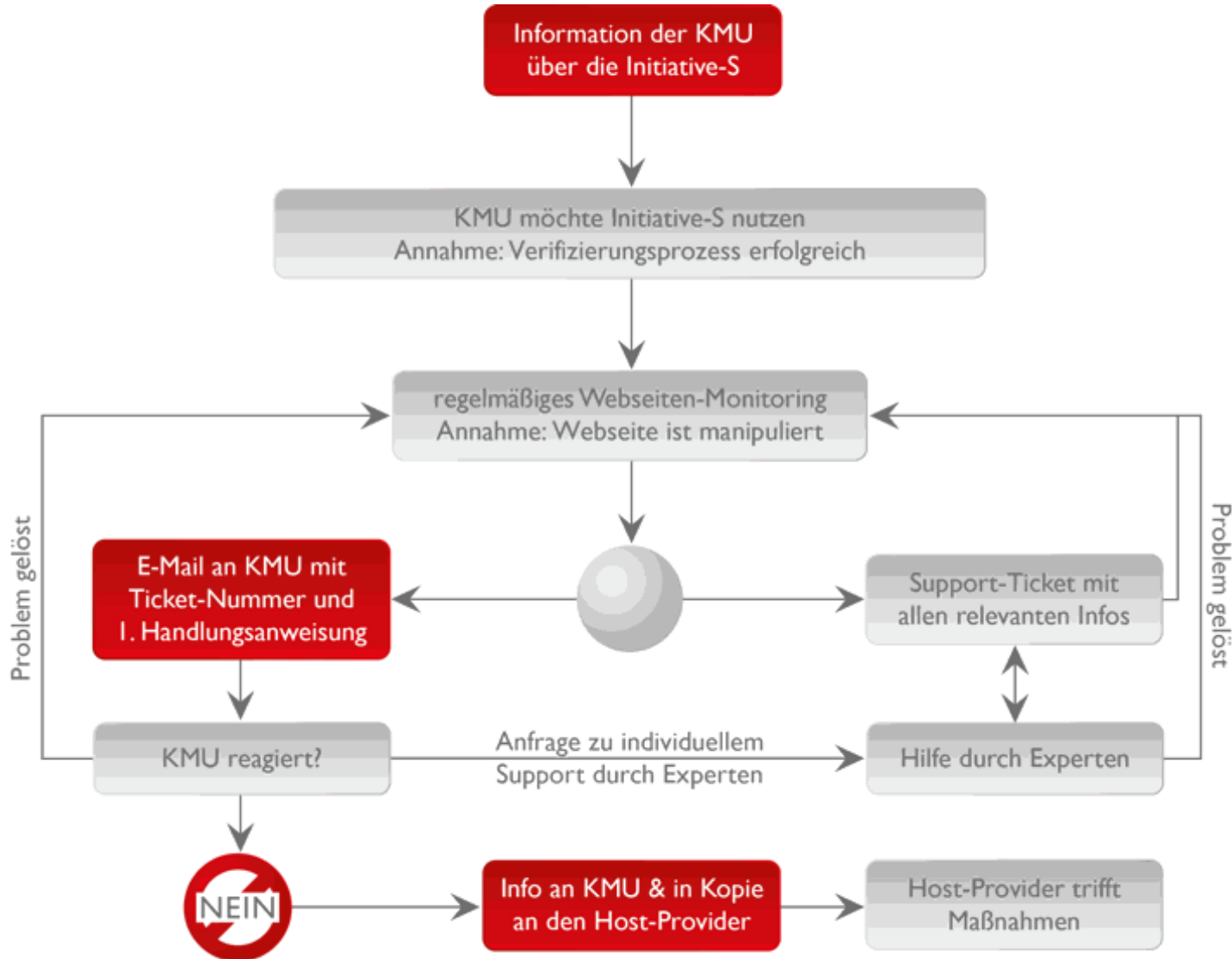
Damit wir Sie im Falle einer Manipulation Ihrer Webseite per E-Mail darüber informieren können, haben Sie die Wahl zwischen folgenden E-Mail-Adressen:

- info@eco.de
- webmaster@eco.de
- abuse@eco.de
- initiative-s@eco.de

**Bitte beachten Sie:** Sollten Sie keine der genannten E-Mail-Adressen registriert haben, legen Sie diese bitte an, bevor Sie die Anmeldung abschließen! Sollten Sie hierbei Unterstützung benötigen, wenden Sie sich bitte an Ihren Hosting-Provider.

[Anmeldung abschließen](#) [Abbrechen](#)

TASK FORCE  
IT - SICHERHEIT IN DER WIRTSCHAFT  
Mehrwert und Schutz für Rechner.



## Zusammenarbeit von botfrei.de und Initiative-S

- Weniger infizierte Webseiten → weniger Infektionen mit Schadprogrammen über Drive-by-Download
- Infizierte Webseiten werden auch von eigenen Mitarbeitern besucht → Infektionen im eigenen Netz
- Durchbrechen des ewigen Kreislaufs!

## Wozu ein Beratungszentrum für KMUs?

- KMUs vernachlässigen Ihre Webauftritte (in Bezug auf Sicherheit)
- Keine eigenen IT-Spezialisten im Haus, kein Verständniss für derartige Sicherheitsaspekte
- 80% aller Schadsoftware wird über giftige Webserver verteilt
- 85% aller verseuchten Webseiten werden auf „regulären“ Webservern gehostet (Quelle: Websense)



**TASK FORCE**  
**IT - SICHERHEIT IN DER WIRTSCHAFT**  

---

**Mehrwert und Schutz für Rechner.**

Gefördert durch:



aufgrund eines Beschlusses  
des Deutschen Bundestages

## Ziele der Initiative-S

- KMUs beim Thema Internetsicherheit unterstützen
- Anzahl der infizierten Webserver in D verkleinern und Infizierte Rechner von Schadprogrammen befreien
- Cyberkriminellen die Grundlage entziehen



## Was macht die Initiative-S?

- hilft betroffenen KMUs, Schadprogramme von ihren Webseiten zu entfernen
- arbeitet mit Hosting-Providern und Anti-Viren-Software-Herstellern zusammen
- Zielgruppe: vor allem kleine und mittelständische Unternehmen



**TASK FORCE**  
**IT - SICHERHEIT IN DER WIRTSCHAFT**  
Mehrwert und Schutz für Rechner.

Gefördert durch:



aufgrund eines Beschlusses  
des Deutschen Bundestages

## Rahmenbedingungen

- Beginn Projektaufbau Juni 2012
- Operativer Projektstart September 2012
- Projektförderung durch BMWi
- eco ist Projektmanager dieser Initiative
- Beirat stellt technische Sachkompetenz bereit und unterstützt eco
- ISPs (Hoster) unterstützen diese Initiative (Kunden informieren...)



## Statistik

- Betaphase (11.9. – 31.12.2012)
  - 3.902 Domains im System erfasst
  - 15 Webauftritten Schadsoftware gefunden
  - diese konnten erfolgreich entfernt werden
- 
- Infrastruktur der Initiative-S ist nach Abschluss der Betaphase in der Lage, täglich 30.000 - 300.000 Webseiten (abhängig von der Anzahl der Unterseiten) zu scannen



**TASK FORCE**  
**IT - SICHERHEIT IN DER WIRTSCHAFT**  
-----  
Mehrwert und Schutz für Rechner.

Gefördert durch:



aufgrund eines Beschlusses  
des Deutschen Bundestages

# **Cornelia Schildt**

## **Projektmanagerin IT-Security**

**Lichtstr. 43h**  
**50825 Köln**

**Tel.: 0221 / 70 00 48 – 0**  
**Fax: 0221 / 70 00 48 – 111**

**cornelia.schildt@eco.de**  
**www.eco.de**  
**www.botfrei.de**  
**www.initiative-s.de**