Bürgerpartei GL
Martin Panzer
Zu den Sieben Zwergen 8
51469 Bergisch Gladbach

BÜRGER
PARTEI GL

Stadt Bergisch Gladbach
Ausschuss für Anregungen und Beschwerden
Konrad Adenauer Platz 1
51465 Bergisch Gladbach

Montag, 15. September 2014

Antrag zum Schutz vor Cyberkriminalität
gem. § 25 GO NRW

Sehr geehrte Damen und Herren,

beigefügten Antrag bitten wir auf die Tagesordnung des Ausschusses für Anregungen und Beschwerden zu setzten als gemeinsamen Antrag.

Mit herzlichen Grüßen

Martin Panzer

Frank Samirae

Antrag

Die Stadt Bergisch Gladbach nimmt am Webseiten Check der Initiative-S, gefördert durch das Bundesministerium für Wirtschaft und Technologie, teil. Sie schützt damit künftig alle städtischen Internetseiten und die Bürger, die diese besuchen vor den Angriffen von Cyber-Kriminellen.

Sachdarstellung

Deutsche Internetseiten gehören zu den beliebtesten Opfern von Cyber-Kriminellen. Weltweit stammen zwölf Prozent aller Webressourcen, welche Schadprogramme wie z.B. Computerviren ausliefern aus Deutschland. Bürger, die solche Internetseiten besuchen um sich bei ihnen zu informieren, infizieren so vielleicht ihre Rechner mit Schadcode wie z.B. Viren und Trojanern. Die Rechner der Opfer können sogar in der Folge Teil eines sogenannten Bot-Netzwerkes werden und unbemerkt zum Versenden von Spam- und Phishing-Mails, oder gar zur Wirtschaftsspionage missbraucht werden.

Die Verantwortung hierfür und die Konsequenzen eines Cyberangriffes würde der Betreiber der Internetseite, von welcher die Infektion ausgeht tragen. In diesem Falle wäre das die Stadt Bergisch Gladbach. Die Schutzmaßnahmen der Inititative-S sind für den Bürger und die Stadt Bergisch Gladbach kostenfrei.

Leider sind in der Vergangenheit Cyberattacken auch in Bergisch Gladbach auf die Internetseite der Stadt erfolgreich von Kriminellen ausgeführt worden. Betroffen war aktuell sogar der Facebook-Account eines stellvertretenden Bürgermeisters. Ebenfalls konnte der Lokalpresse entnommen werden, wie die Internetseiten von größeren Vereinen gehackt werden konnten.

Die kostenfreie Möglichkeit mit dem Webseiten Check der Initiative-S einen erfolgreichen Cyberangriff frühzeitig zu erkennen und die Bürger zu schützen, mindert Haftungsrisiken für die Stadt und schützt so die knappen Mittel des Haushalts.

Martin Panzer

Frank Samirae

Anlagen:

- *Flyer und Screenshot der Inititiave-S*
- *Trojaner auf Homepage der Stadt?, Kölnische Rundschau vom 24.04.2008*
- *Facebook-Account des Vize-Bürgermeisters Willnecker Opfer von Hacker-Angriff, Kölner Stadtanzeiger vom 09.09.2014*
- *Berichte zum Hacker Angriff auf die Internetseiten der St. Sebastianus Schützenbruderschaft:*

  Spaßvogel schießt Homepage der St. Sebastianus Schützenbruderschaft Schildgen ab GL Aktuell vom 17.08.2014
  http://www.glaktuell.net/spassvogel-schiesst-hp-ab/

  Schildgener Schützen Im Griff von Zombie-Hacker, Kölner Stadtanzeiger vom 18.08.2014

Wozu die Initiative-S?

Deutsche Internetseiten gehören zu den beliebtesten Zielen von Cyber-Kriminellen: „Zwölf Prozent aller Webressourcen, die Schadprogramme ausliefern, stammen aus Deutschland." (Quelle: Kaspersky)

Demnach besteht eine große Wahrscheinlichkeit, dass Ihre Internetseiten davon betroffen sind. Kunden und Interessenten, die sich online bei Ihnen informieren, infizieren so vielleicht ihre Rechner mit Schadcode wie Viren und Trojanern. Oder die Rechner werden Teil eines sogenannten Bot-Netzwerks und unbemerkt zum Versenden von Spam- und Phishing-Mails oder sogar für DDoS-Attacken und Wirtschaftsspionage missbraucht.

Die Verantwortung dafür tragen Sie, und die Konsequenzen können weitreichend sein:
Sie haften für Fremdschäden, und Ihre Webseiten-Besucher können rechtliche Schritte gegen Sie einleiten. Möglicherweise werden Ihre lokalen Rechner infiziert und Ihre Internetseiten durch Ihren Provider oder Suchmaschinen wie Google blockiert. Der Imageverlust und der wirtschaftliche Schaden können zum Ruin führen.

Die Initiative-S informiert kleine und mittelständische Unternehmen über die Gefahr, die vielen nicht bewusst ist. Nach dem aufwändigen Erstellen des Webauftritts verlieren sie das Thema oft aus den Augen und werden so zum idealen Cyber-Opfer. Die Experten der Initiative-S unterstützen sie dabei, ihre Internetseiten regelmäßig zu überprüfen, von Schadsoftware zu befreien und nachhaltig gegen neue Angriffe zu schützen – und das kostenfrei.

Initiative-S: Gemeinsam stark

Eine Initiative des

eco

Verband der deutschen Internetwirtschaft e.V.

eco – Verband der deutschen Internetwirtschaft e.V.
Lichtstraße 43h
50825 Köln
www.initiative-s.de
kontakt@initiative-s.de

Gefördert durch:

Bundesministerium für Wirtschaft und Technologie

aufgrund eines Beschlusses des Deutschen Bundestages

Bundesministerium für Wirtschaft und Technologie
Scharnhorststraße 34-37
10115 Berlin
www.bmwi.de

Im Rahmen der

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

Task Force „IT-Sicherheit in der wWirtschaft"
Die Initiative des BMWi will gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung vor allem kleine und mittelständische Unternehmen für IT-Sicherheit sensibilisieren und dabei unterstützen, die Sicherheit der IKT-Systeme zu verbessern.
www.it-sicherheit-in-der-wirtschaft.de

Mit Unterstützung diverser Hosting-Provider und Hersteller von Antiviren-Programmen.

eco

Verband der deutschen Internetwirtschaft e.V.

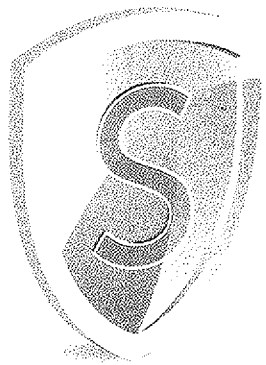
Gefördert durch:

Bundesministerium für Wirtschaft und Technologie

aufgrund eines Beschlusses des Deutschen Bundestages

INITIATIVE S

Der Webseiten-Check zur Sicherheit Ihres Internetauftritts



www.initiative-s.de
von den Experten der Initiative S getestet

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

Seiten-Check

Domain eingeben, verifizieren und los geht's

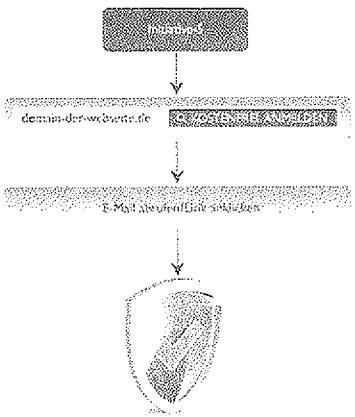
Liefern ihre Internetseiten Schadcode aus, kann Sie das teuer zu stehen kommen. Ihre Teilnahme am Webseiten-Check kostet hingegen lediglich ein kleines bisschen Zeit und ist ganz einfach:

1. **www.initiative-s.de** besuchen,
2. die zu überprüfende Internetadresse sowie eine gültige E-Mail-Adresse eingeben,
3. im Posteingang zur Validierung die E-Mail der Initiative-S bestätigen.

Anschließend überprüfen die Sicherheitsexperten Ihren Webauftritt auf Schadprogramme – und zwar in regelmäßigen Abständen, damit er jetzt und künftig sauber ist.

Hierfür kommen sowohl diverse namhafte Antiviren-Programme zum Einsatz als auch eigene Entwicklungen, um eine hohe Erkennungsrate zu gewährleisten. Ihr System wird dabei nicht belastet.

Selbstverständlich können Sie diesen Service jederzeit wieder stoppen. Klicken Sie hierzu einfach auf den Abmelde-Link in unserer Verifizierungs-E-Mail oder in unseren E-Mail-Reportings.



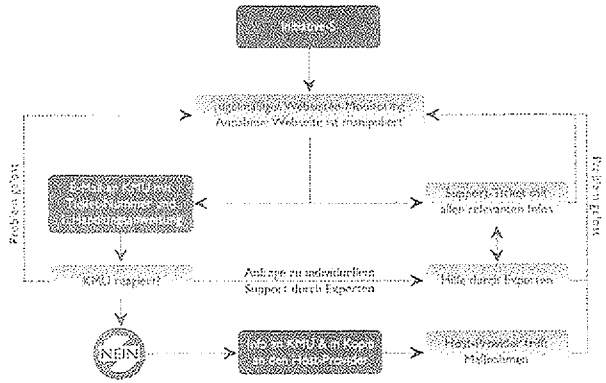
Säubern

Schadcode entfernen mit individuellem Support

Entdecken die Sicherheitsexperten eine Infektion, erhalten Sie in einer E-Mail erste Informationen zur Bereinigung Ihrer Webseiten und im Bedarfsfall der Firmenrechner. Unter www.initiative-s.de stehen dann detaillierte Anweisungen und Tools bereit.

Zusätzlich enthält die E-Mail eine Ticket-Nummer und Kontaktdaten zu den Experten der Initiative-S, die für Rückfragen zur Verfügung stehen sowie bei der Analyse und der Problembehebung helfen.

Beim erneuten Check überprüfen die Experten, ob die Infektion beseitigt wurde. Wenn ja, erhalten Sie eine Bestätigung mit Hinweisen zur Prävention. Ist der Schadcode immer noch online, werden Sie erneut informiert und darüber hinaus Ihr Provider.



Schützen

Wege zum sicheren Internetauftritt

Das Entfernen der Schadprogramme ist gut und schön. Doch was nützt das, wenn es gleich wieder zu einer Infektion kommt?

Um das zu verhindern, analysieren die Experten der Initiative-S beim Webseiten-Check auch die Ursachen und geben Tipps, wie Sie diese künftig vermeiden können.

Empfohlene Schutzmaßnahmen sind:

- eigene Server regelmäßig aktualisieren,
- nicht benötigte Server-Dienste abschalten,
- die Software Ihres Internetauftritts sowie Fremdprogramme aktuell halten,
- eine Web Application Firewall vorschalten,
- starke Passwörter wählen und diese regelmäßig ändern,
- nicht benötigte Benutzerkonten deaktivieren
- und natürlich eine regelmäßige Überprüfung auf Schadcode, die gerne die Initiative-S für Sie übernimmt!

Zudem ist es wichtig, dass Sie Ihr Firmennetz regelmäßig auf Virenbefall prüfen. Unter **www.botfrei.de** stellen wir neben unseren DE-Cleanern weitere nützliche Tools vor, die auch für den Einsatz im gewerblichen Umfeld geeignet sind.

INITIATIVE S

Eine Initiative von eco

Gefördert durch

Mit Unterstützung von

Startseite Schützen Säubern Über das Projekt Teilnehmer Kontakt

Vorbeugen. Untersuchen. Sicherheit genießen.

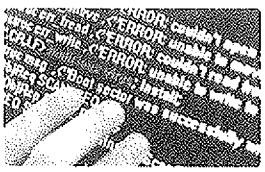
Schützen Sie Ihren Webauftritt und Ihre Besucher vor unbemerkten Manipulationen und erhalten Sie professionelle Hilfe.
Geben Sie hier den Namen Ihrer Internetadresse ein und registrieren Sie sich kostenlos.

KOSTENFREI ANMELDEN

SEITENCHECK

SÄUBERN

SCHÜTZEN



Herzlich willkommen beim Seiten-Check der Initiative-S!

Mehr als die Hälfte aller Cyber-Angriffe weltweit betreffen nach Symantecs 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.

IT-Sicherheit IN DER WIRTSCHAFT

Roadshow Initiative S

Der kostenlose Webseiten-Check zur Sicherheit Ihres Internetauftritts geht auf Tour.

- 12. - 13.09.2014
  JoomlaDay, Köln

Kölnische Rundschau

Rhein-Berg - 24.04.2008

Trojaner auf Homepage der Stadt?

Detlev Nicolin aus Paffrath traute seinen Augen nicht: Da ging er gestern Abend auf die Internetseite der Stadt Bergisch Gladbach und fing sich vier Trojaner ein...

RHEIN-BERG. Detlev Nicolin aus Paffrath traute seinen Augen nicht: Da ging er gestern Abend auf die Internetseite der Stadt Bergisch Gladbach und fing sich vier Trojaner ein. Diese aggressiven Computerprogramme, die ohne Wissen des Anwenders schädliche Funktionen ausführen, wurden zwar sofort von seinem Virenschutz-Programm entschärft, aber so etwas auf einer städtischen Seite - das ist schon heftig, ärgerte sich der Student. Ein Rundruf bei Freunden bestätigte: Auch sie meldeten Trojaner von der Stadt-Homepage.

Bei der Firma Oevermann Networks, die die Seite betreut, schrillten da bereits die virtuellen Alarmglocken. Wie die Gladbacher Internetseite habe man kurz nach 18 Uhr auch die ebenfalls betreuten Internetauftritte von Rösrath, Overath, Odenthal und vom Kreis vorsichtshalber stillgelegt, sagt Dieter Porzberg, einer der Geschäftsführer, auf Anfrage.

Ursache des Problems? In einem Artikel, der auf mehreren Seiten aufgerufen werden konnte und den offenbar einer der Redakteure in den Kommunen online gestellt hatte, befand sich ein eingebetteter Link auf eine chinesische Seite. Von der konnte sich der Internetnutzer dann den Trojaner einfangen. Wer den Artikel ins Netz gestellt hat, war gestern Abend noch unklar. Nach und nach wurden die Homepages wieder online gestellt. (wg)

Artikel URL: http://www.rundschau-online.de/rhein-berg/trojaner-auf-homepage-der-stadt-,16064474,15582208.html

Kölner Stadt-Anzeiger

Bergisch Gladbach - 09.09.2014

FACEBOOK-ACCOUNT DES VIZE-BÜRGERMEISTERS

Willnecker Opfer von Hacker-Angriff

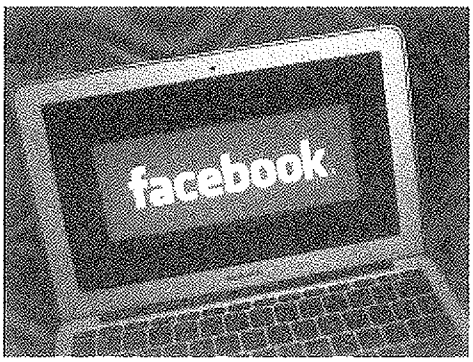


Foto: REUTERS

Von Guido Wagner

Der Facebook-Account des Vize-Bürgermeisters, Joseph Willnecker, wurde gehackt. In seinem Namen haben Unbekannte seine Facebook-Freunde aufgefordert, Geld zu überweisen. Er hat Anzeige erstattet. Das LKA ermittelt

Dass sein Mobiltelefon am Montagabend bei einer Ausstellungseröffnung ständig in der Tasche vibrierte, kam Gladbachs Vize-Bürgermeister Josef Willnecker schon merkwürdig vor. Doch als offizieller Repräsentant der Kreisstadt konnte er da unmöglich ans Telefon gehen. Hätte er geahnt, dass Verbrecher kurz zuvor in seinem Namen versucht hatten, Geld zu erbeuten – er wäre vielleicht doch vor die Türe gegangen.

500 EURO GEFORDERT

„Jemand hat meine Seite bei Facebook kopiert, sich mit meinem Namen ausgegeben und 500 Euro von Leuten gefordert, die mit mir in dem Netzwerk befreundet sind", berichtet der Vize-Bürgermeister gestern auf Anfrage dieser Zeitung immer noch sichtlich erschüttert. „Einfach erschreckend, die Leute, die mich während der Ausstellung angerufen haben, hatten das durchschaut und wollten mich warnen."

Nach der Veranstaltung informierte Willnecker umgehend seine Facebook-Kontakte, stellte klar, dass die Aufforderungen zur Geldüberweisung vom Abend nicht von ihm stammten. Via Nachrichten-Plattform hatte der bislang unbekannte Hacker im Namen Willneckers und mit dessen Profilbild mehrere Bekannte des Vize-Bürgermeisters angeschrieben und darum gebeten, ihm per elektronischem Zahlungsmittel, sogenannten Paysafe-Karten, Geld zukommen zu lassen. Am Dienstagmorgen werde er dann das Geld „und einen kleinen Aufschlag" zurückzahlen.

Die Begründung des Unbekannten im Namen Willneckers: Er müsse gerade etwas im Internet kaufen, habe aber die notwendigen Transaktionsnummern für die Sofortüberweisung nicht dabei. Ob jemand dieser obskuren Zahlungsaufforderung gefolgt ist, war gestern noch unklar. Willnecker allerdings erstattete umgehend Anzeige wegen Betrugsverdachts und Rufschädigung bei der Kriminalpolizei. Der Fall sei als Computerbetrug aufgenommen worden, bestätigte Polizeisprecher Peter Raubuch gestern Nachmittag auf Anfrage.

UNGEWÖHNLICHES VERFAHREN

Die kriminelle Masche, ein Profil in Facebook zu kopieren und dann via Nachrichten-Plattform „WhatsApp" auf elektronischem Weg Geld zu erbeuten, sei den Experten der Kreispolizei bislang noch

nicht untergekommen, so Raubuch. Die Experten vom Landeskriminalamt wollen sich auf Anfrage dieser Zeitung voraussichtlich heute zu dem Fall äußern. Josef Willnecker sitzt der Schock in den Knochen: „Ich muss jetzt sehen, wie ich das sperren kann."

Artikel URL: http://www.ksta.de/bergisch-gladbach/facebook-account-des-vize-buergermeisters-willnecker-opfer-von-hacker-angriff,15189226,28359002.html

Aktuelles, Blaulicht, Schildgen

Spaßvogel schießt Homepage der St. Sebastianus Schützenbruderschaft Schildgen ab

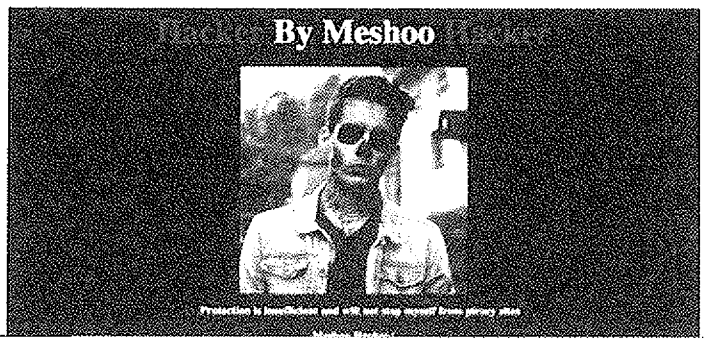
Vorlesen

Besucher die sich für Brauchtum und Schützenwesen interessieren, finden derzeit auf den Internetseiten des Schützenverein Schildgen keine tiefen Informationen vor. Lediglich eine Zombie Figur ist hier abgebildet. Offensichtlich hat man den Schutz vor Gefahren in der digitalen Welt nicht ernst genommen. Die Redaktion des Portals GL-Aktuell.net hat bereits den Vereinsvorstand informiert. Eine Rückmeldung ob wann das Problem behoben werden kann steht noch aus.

Frank Samirae Geschäftsführer des gleichnamigen EDV-Unternehmens in Bergisch Gladbach und neues Ratsmitglied nimmt hierzu Stellung: „Wir sehen die Entwicklung mit großer Sorge. Wer im digitalen Zeitalter schläft, wacht irgendwann unangenehm auf. Wir stellen zunehmend auch Angriffe auf Firmen- und Heimnetzwerke fest. Viele Netzwerke und Computer sind heute nur noch unzureichend geschützt."

Der Verfall passt ins Bild. Die flächendeckende Internet-Überwachung durch US-Geheimdienste ist ein Jahr nach den ersten Enthüllungen immer noch ein Thema. „Die digitale Gefährdungslage für Unternehmen, Vereine und auch die öffentlichen Träger stellt grundsätzlich bedenklich", fasst Frank Samirae zusammen.

„Auch wenn in der öffentlichen Wahrnehmung die größere Bedrohung von Spionage-Attacken ausländischer Staaten ausgeht, sind es kriminelle Hacker, die uns im Tagesgeschäft die meisten Sorgen machen." – schließt Samirae. Nach wie vor stellen Online-Kriminelle eine wesentliche Bedrohung dar. Prominentes und jüngstes Beispiel im Bergischen Land ist der seit heute bekannte Hack der Homepage St. Sebastianus Schützenbruderschaft Schildgen.



POPULAR

- Kölner Pussy Riot Aktivisten konfrontieren orthodoxe Kirche
- Pro Pussy Riot Flashmob vor Deutschlands einzigem russisch-orthodoxem Pilgerzentr Bekannt
- Mord in Bergisch Gladbach: Kripo sucht 2 Tatverdächtigen
- Lucke (AfD) kommt nach Bergisch Gladba
- Alternative für Deutschland in Bergisch Gl bald im Stadtrat?

CATEGORIES

ARCHIVES

Suche nach:

Suche

LETZTE BEITRÄGE

Kulturstrolche-Projekt erstmals in Bergisch Gladbach

S-Bahnhof bekommt mehr Kurzzeit- und Behindertenparkplätze

Bergische Erzählkonzerte gehen in die nächste Saison

INFORMATIC

Premium News

Designed by A

Anmelden

Powered by W

Entries RSS

Comments RS

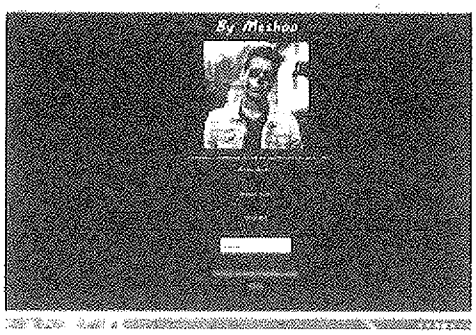
Kölner Stadt-Anzeiger

Bergisch Gladbach - 18.08.2014

SCHILDGENER SCHÜTZEN

Im Griff von Zombie-Hacker

Von Daniela Fobbe-Klemm



Bei diesem Bild erkennt man sofort: Hier handelt es sich nicht um einen Schildgener Schützen. Die Seite wurde gehackt. Foto: privat

Auf der Homepage der Schildgener Schützen empfängt den Besucher eine Zombiefratze. Ein Hacker namens Meshoo hat die Internetseite lahmgelegt. Über die Ursache kann bisher nur spekuliert werden.

Die Schildgener Schützen sind offline. Ihre Internetseite ist gehackt worden. Wer derzeit auf die Homepage klickt, könnte denken, es ist schon Halloween. Eine Zombiefratze erscheint dort, verbunden mit dem lakonischen Hinweis, dass die Seite von einem sich Meshoo nennenden Hacker geknackt wurde und ihr Schutz mangelhaft sei.

Jetzt gibt es ja Menschen, für die Schützenfeste gleichbedeutend mit Horrorvorstellungen sind. Aber dass die traditionsbewussten Schützen sich jemanden derart zum Feind gemacht haben, dass er sich die Mühe macht, ihre Seite lahmzulegen, ist schwer zu glauben. Schließlich ist das Schützenfest 2014 bereits gefeiert. Wer sich also Anfang Juli darüber geärgert hatte, am sehr frühen Sonntagmorgen mit Böllerschüssen geweckt zu werden, sollte sich wieder abgeregt haben.

Arabische Schriftzeichen im Tab lassen die Vermutung zu, dass es sich um einen Angriff aus dem Ausland handelt. Wer könnte also hinter der virtuellen Attacke stecken? „Vermutlich die NSA", mutmaßt der erste Vorsitzende der Schildgener Schützen, Peter Koch, mit einem Augenzwinkern. Am vergangenen Freitag war er über den Hackerangriff informiert worden. So richtig ernst kann er den Vorfall aber auch am Montag nicht nehmen. „Wir sind doch nur ein Schützenverein, wer interessiert sich denn für unsere Seite?", fragt er ungläubig.

Zusammenhänge mit der aktuellen Diskussion über den Umgang von Schützenbruderschaften mit andersgläubigen Mitgliedern oder gar muslimischen Schützenkönigen sind zwar denkbar, aber kaum zu beweisen. Auch die emotional geführte Diskussion über den Schießstand am 2012 von den Schützen übernommenen Schildgener Bürgerzentrum ist weitgehend beendet. Und so bleiben nur Spekulationen über die Ursache des Hackerangriffs. War es ein Krimineller? Der wird auf der Seite wohl kaum Verwertbares wie etwa Kreditkartendaten gefunden haben. Und um ein Virus zu verbreiten, gibt es sicher Seiten mit mehr Zugriffen pro Tag.

Vielleicht war es aber schlicht ein Irrtum. Denn wer sich im Internet mal die Hackerangriffe, von denen der bei Twitter und Youtube sehr martialisch aussehenden Meshoo behauptet, dahinter zu stecken, anschaut, der findet keine anderen deutschen Seiten. Aber viele aus Amerika, Singapur oder dem Iran. Vielleicht hat der Mann sich schlicht vertan und geglaubt, er hätte irgendeine rivalisierende Gang aus dem Verkehr gezogen. Und sollte es doch die NSA gewesen sein, haben die amerikanischen Spione wohl kaum neue Erkenntnisse über die Deutschen im Allgemeinen und die Gladbacher im Besonderen

gewinnen können.

www.schuetzenverein-schildgen.de

Artikel URL: http://www.ksta.de/bergisch-gladbach/schildgener-schuetzen-im-griff-von-zombie-hacker,15189226,28156574.html