06
Nov./Dez.
2023

68. Jahrgang
A 5625 | € 7,50
ISSN (Print) 0722-5962
www.pvtweb.de

pvt

POLIZEI VERKEHR + TECHNIK

Seit 1956 die Fachzeitschrift für Innere Sicherheit

Voller Einsatz

Seiten 6-23

INSPECTION – Gezieltes Finden gehackter Webseiten

Joachim Feist

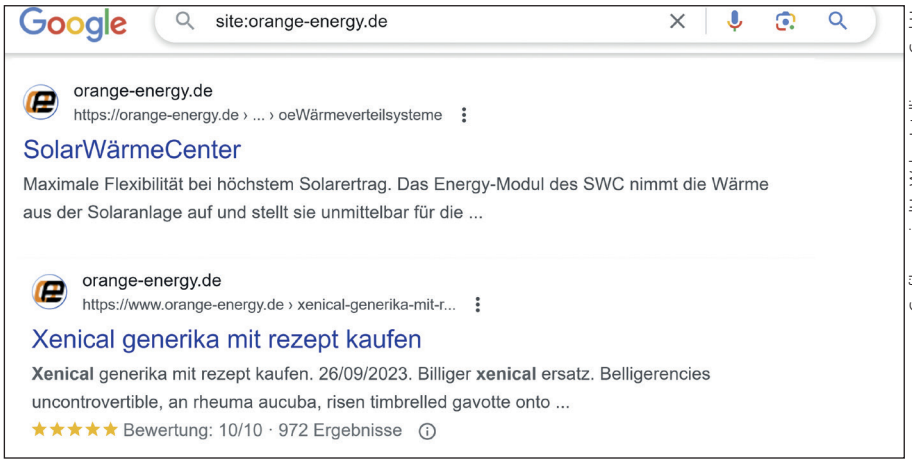
Webseitenhackings werden im Projekt INSPECTION automatisiert von außen erkannt. Dadurch können die Verursacher gezielter identifiziert, die Betroffenen zielgerichtet informiert und Prävention entlang von Beispielen plastisch gemacht werden.

Gehackte Webseiten von außen erkennen

Das Projekt INSPECTION (www.web-inspection.de) verfolgt das Ziel, gehackte Webseiten durch das maschinelle Durchsuchen des deutschsprachigen Internets von außen zu identifizieren. Die Straftat des Hackings wird demnach nicht vom Betroffenen erkannt, sondern im größeren Kontext mit Hilfe lernender Verfahren automatisiert ermittelt und weitergemeldet. Auf diese Weise konnten bereits 10.000 Hackingfälle über die verschiedensten Branchen hinweg automatisiert gefunden werden. Dies erlaubt zum einen, Spuren zu den Straftätern besser zu ermitteln, zum anderen liefern die Fälle wertvolles Anschauungsmaterial für die Prävention. Lokale Beispiele oder Beispiele bestimmter Branchen können für Veranstaltungen und Informationsmaterial herangezogen werden, um Zuhörer zum Handeln zu motivieren.

Die Erkennung des Webseiten-Hackings von außen ist möglich, weil die Betrüger die gute Positionierung bestehender Seiten nutzen, um mit manipulierten Inhalten auf missbräuchliche Angebote wie Fake-Shops, Ransomware-Downloads, Bitcoin-Portale, Phishing, Pornographie und Casino-Seiten weiterzuleiten. Der Webauftritt bleibt dabei aus Nutzersicht unauffällig, d.h. die normale Verwendbarkeit der Webseite bleibt erhalten. Deshalb fallen die Hackings den Betroffenen über Monate, häufig sogar Jahre, nicht auf.

Den Mechanismus kann man nachvollziehen, wenn man in der Suchmaschine mit dem Parameter site: sämtliche von der Suchmaschine indexierten Seiten einer betroffenen Domain auflisten lässt. Im Beispiel der Suche „site:orange-energy.de“ (Abbildung 1) erscheinen neben den regulären Einträgen zu Energiesystemen manipulierte Einträge der Hacker zu Arzneimitteln. Diese sind



Grafiken: mindUp Web + Intelligence GmbH

Abbildung 1: Eine gehackte Webseite weist neben regulären Einträgen manipulierte Seiten auf, die zu einem Fakeshop führen.

für die Suchmaschine optimiert und zeigen sogar positive Bewertungen an. Ein Klick auf einen solchen Eintrag führt Verbraucher, die das Abnehm-Medikament suchen, über eine Weiterleitung in einen Fake-Shop.

Bestehende Webseiten mit Sicherheitslücken sind das Ziel der Hacker. Die thematische Nähe zu den Themen der Zielseiten spielen dabei eine untergeordnete Rolle. Die Hacker belassen die originalen Inhalte der Webseite und ergänzen Ihre Themen zusätzlich als neue Seiten der Domain. Sie erreichen damit eine sehr schnelle und gute Suchmaschinenplatzierung. In Einzelfällen gelingt es den Angreifern eine sechsstellige Zahl zusätzlicher Unterseiten in einen bestehenden Webauftritt einzuhängen. Damit wird die manipulierte Webseite Suchmaschinen in guten Positionen zu den verschiedensten Themen der Zielseiten der Hacker gefunden.

Sollte der Fake-Shop durch Markeninhaber oder polizeiliche Ermittlungen geschlossen werden, wird einfach eine neue Internet-Domäne angemeldet und die Phalanx manipulierter Webseiten entsprechend aktualisiert, um direkt vom ersten Tag an, Besucher auf neue missbräuchliche Ziele zu lenken. Die Hacker haben Vollzugriff auf die Internet-Domänen und können dadurch weitere betrügerische Nutzungsformen wie Spam-Versand oder Angriffe auf andere Rechner implementieren.

Permanente Überwachung neuer Sucheinträge mit KI

Die mindUp Web + Intelligence GmbH ist im Forschungsprojekt INSPECTION zuständig für das Finden der gehackten Webseiten. Die Analysemethoden von mindUp basieren auf der permanenten Auswertung von sehr großen Mengen von Suchergebnissen der Suchmaschinen. Gesucht wird in der ganzen begrifflichen Breite des Online-Shoppings und zusätzlich mit Begrifflichkeiten häufiger Missbrauchsthemen wie Kryptowährungen, Casinos und Erotik. Mit Techniken der künstlichen Intelligenz bezüglich verschiedener Auffälligkeiten werden die betrügerischen Inhalte erkannt und von normalen Ergebnissen unterschieden.

Zusätzlich zur permanenten Suche in den Suchmaschinen werden proaktiv Webseiten

der im Projekt beteiligten Handwerkskammern und Fachverbände gecrawlt, um in der regionalen und thematischen Struktur „anlasslos“ Problemfälle zu finden und über die direkten Beziehungen der Verbände anzusprechen.

Fallbündelung für die Strafverfolgung

Bei den entdeckten Straftaten handelt es sich bei den Webseitenhackings um „Cybercrime im engeren Sinne“, bei den Zielseiten um Betrug, in Teilbereichen um Verstöße gegen das Arzneimittelrecht, da rezeptpflichtige Arzneimittel ohne Verschreibung angeboten werden. Für die Strafverfolgung sind diese Straftaten in der Regel schwer zu ahnden, da sie verteilt auf sechzehn Bundesländer bei den ZACs oder Polizeidienststellen gemeldet werden. Häufig bleibt die Anzeige der Betroffenen auch aus, da diese den Vorfall nicht bemerken oder nicht nach außen dringen lassen möchten.

Die Erkennung von außen im großen Stil und die Bündelung über das gleichartige Hackingziel bieten die Möglichkeit, Ermittlungen der Straftäter zusammenzulegen und aus der Summe der Spuren eine bessere Sicht auf die Täterschaft zu gewinnen. So wurden die Universitäten München und Kiel vom gleichen Verursacher gehackt (Abbildung 2).

Webseitenhacking als Zulieferer zu Fake Shops, Scareware und Ransomware

Zu Projektbeginn lag der Fokus darauf, gehackte Webseiten zu finden, die auf Fake-Online Shops verlinken. Im Verlauf des Projektes wurde klar, dass diese Form des Hackings auch für andere Missbrauchsformen wie Pornographie, Ransomware Downloads, illegales Glücksspiel, Bitcoin-Betrug oder zur Promotion von Hacker-Tools genutzt wird.

Es wird als Technik auch nicht immer Hacking eingesetzt. Stattdessen werden auch in extrem großem Umfang Webseiten angemietet (sog. Satelliten-Seiten), um dann mit den gleichen Techniken wie beim Hacking, Weiterleitungen einzurichten (Abbildung 3).

Logfiles von Hackings legen nahe, dass arbeitsteilig gearbeitet wird. Ein Hacker übernimmt Internet-Domänen, ein SEO-Experte präpariert die Inhalte so, dass Sie von den Suchmaschinen ideal aufgenommen werden. Der dritte Akteur dürfte der Auftraggeber sein, der den Fake-Shop oder das missbräuchliche Portal betreibt. Teilweise sind Strukturen zu entdecken, die ähnlich zu Adservern in der Online-Werbebranche arbeiten, d.h. wirtschaftlich getrennte Zubringerdienste leiten dem Höchstbietenden gewinnmaximiert die Besucher zu.

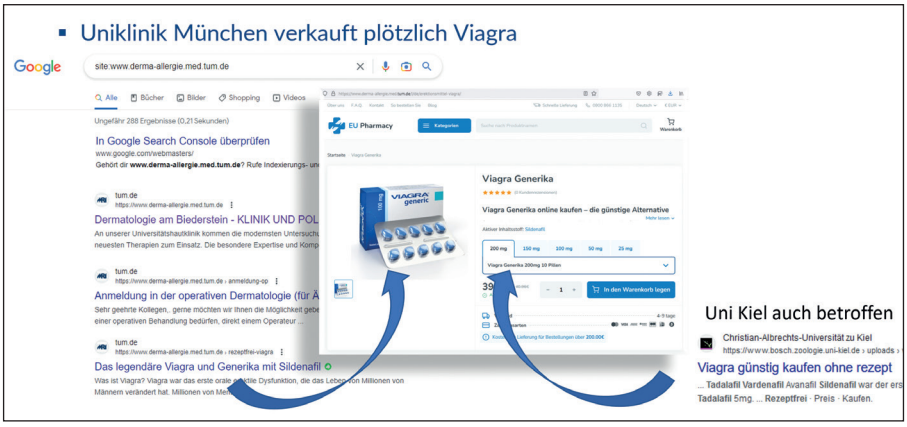


Abbildung 2: Die Analyse erlaubt die Bündelung von Fällen aufgrund des gleichen Verursachers.

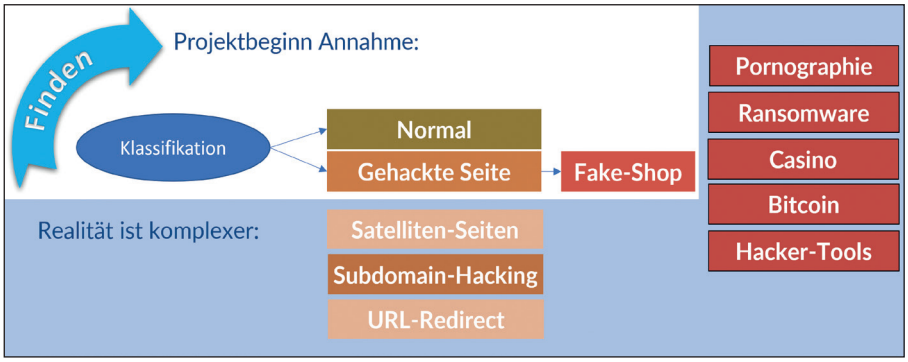


Abbildung 3: Das Webseitenhacking wird für Fake-Shops und viele andere Missbrauchsformen angewandt und taucht in verschiedenen Varianten auf.

Wie können Betroffene gezielt informiert werden?

Neben dem Finden stellt auch das Behandeln eine Herausforderung dar. Zu den Betroffenen zählen Vereine, Blogbetreiber, Handwerker, große Firmen und auch Universitäten.

Fallmeldungen wurden anfangs über die Zentralen Ansprechstellen Cybercrime (ZAC) der Bundesländer geleitet. Dort wurden sie je nach Vorgehen im jeweiligen Bundesland meist dezentral bearbeitet. Als schwierig erwies sich dabei, dass häufig keine Rückmeldung zum INSPECTION-Projekt vorgesehen oder

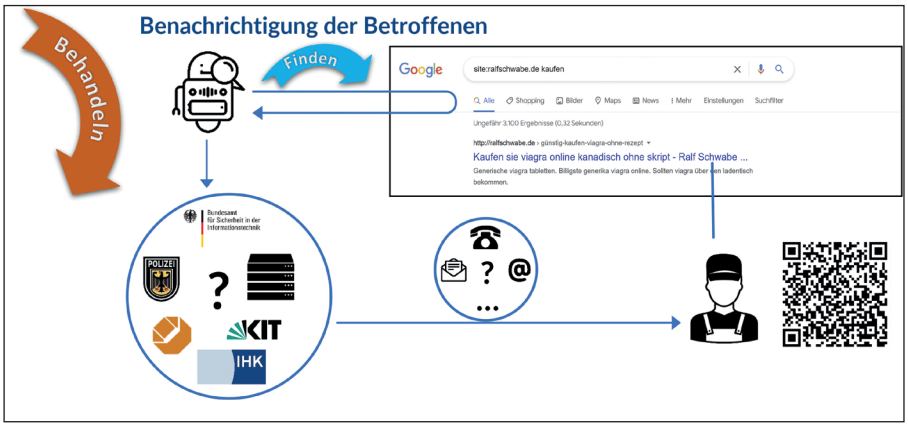


Abbildung 4: Die Information der Betroffenen kann über verschiedene Absender und Kanäle erfolgen. Ein Ansprache-Experiment sucht den effektivsten Weg.

rechtlich zulässig ist. Es blieb dadurch unklar, ob der Fall bearbeitet wurde. In manchen Bundesländern wurde die meldende Person der Firmen im INSPECTION Projekt in der Anzeige geführt, wodurch dann teilweise mehr als zwölf Monate später Informationen über eingestellte Ermittlungsverfahren eingingen.

Diese Herausforderungen im Bearbeitungs-Workflow fielen bereits früh im Projekt auf und wurden daraufhin auch von Studenten der sächsischen Polizeihochschule untersucht, um für eine solche automatisierte Form der Anzeige passende Vorgehensweisen zu erarbeiten. Im Rahmen der Projektlaufzeit konnten allerdings keine neuen Abläufe etabliert werden.

In einem Experiment zur effektiven Ansprache Betroffener wurde daraufhin durch die Forschungsgruppe SECUSO des KIT (Karlsruher Institut für Technologie) untersucht, welcher Absender der Botschaft und welche Inhalte der Botschaften von Organisationen außerhalb der Polizeiorganisation am geeignetsten erscheinen, um die Betroffenen zu einer Behebung der Problematik zu bewegen (Abbildung 4).

In Österreich werden die Fälle durch die Watchlist Internet bearbeitet, in der Schweiz zunächst von der SWITCH, zukünftig vom Nationalen Zentrum für Cybersicherheit. In Deutschland nehmen am Ansprachexperiment zwei Webhoster, das BSI und das KIT selbst teil.

Es konnte dabei ermittelt werden, dass die Information der Betroffenen mit zielgerichteten Informationen wesentlich erfolgreicher ist, als die gehackten Webseitenbetreiber sich selbst zu überlassen. Die höchste Erfolgsquote in der Ansprache weisen zum derzeitigen Auswertungsstand das BSI und ein Webhoster auf, wobei eine technische Botschaft beim Absender BSI am besten wirkt. Eine Botschaft zu drohenden Reputationsschäden ist beim Webhoster am nachhaltigsten bzgl. einer zeitnahen Problembehandlung durch die Betroffenen.

Prävention durch Beispiele

Im Projekt werden auch Präventions-Materialien erstellt. Das erste Video erläutert die generelle Problematik. Ein zweites Video gibt konkrete Hilfestellungen für die Behebung dieser Form des Hackings, welches inhaltlich durch die forensischen Analysen der BDO AG Wirtschaftsprüfungsgesellschaft ermöglich wurde. Diese Unterlagen können nun für Präventionsarbeit von Polizei und Verbänden genutzt werden, um Webseitenbetreiber zu sensibilisieren. Sehr wertvoll ist darüber hinaus der große Schatz an Beispielen Betroffener. Dadurch wird es möglich, mit einer Fülle von regionalen oder branchenbezogenen Beispielen das Thema IT-Sicherheit in konkrete Betroffenheit in der Zielgruppe umzuwandeln.

Abbildung 5: Beteiligte am Projekt INSPECTION

Mithilfe gesucht

Offen ist noch, wie nach Ende des Forschungsprojekts das Finden und das Benachrichtigen am effizientesten fortgeführt werden kann. Weitergehende Ansatzpunkte der aktuellen Arbeit wurden identifiziert und können in zukünftigen Schritten ergründet werden. So könnte das schnelle Erkennen der von den Kriminellen selbst angemieteten Webseiten eine lohnende Zielrichtung sein, indem diese direkt bei Neuanmeldungen von Internet-Domänen durch ein Screening entdeckt werden. Hier gibt es von der EU und ICANN eine Initiative unter dem Namen „DNS Abuse“, um solche Machenschaften einzugrenzen.

Da viele Zielseiten Fake-Online-Shops sind, die Vorkasse verlangen, ist als weiterer Aspekt einer Zusammenarbeit zwischen Polizei und INSPECTION zukünftig auch der Bezahlweg zu berücksichtigen. Mit Crawling-Techniken können die Vorkasse-Zielkonten ermittelt werden. Damit lässt sich der Weg des Geldes verfolgen oder frühzeitig blockieren - bevor große Summen über die Konten der häufig ahnungslosen „Money Mules“ geschleust werden.

Das Projekt INSPECTION (web-inspection.de) ist gefördert im Programm „KMU Innovativ“ des Bundesministeriums für Bildung und Forschung. Initiator ist die mindUp Web + Intelligence GmbH aus Konstanz, weitere Projektträger sind das Karlsruher Institut für Technologie – Forschungsgruppe SECUSO und die Forensikexperten der BDO AG Wirtschaftsprüfungsgesellschaft.

Das Projekt läuft seit Juni 2020 unter internationaler Beteiligung durch die Swiss Internet Security Alliance (SWITCH, Nationales Zentrum für Cybersicherheit) und der Watchlist Internet aus Österreich. Das Projekt wird von Webhostern und Verbänden unterstützt.

Das INSPECTION Projekt endet in 2023 – Ideen zur Fortführung gerade zusammen mit den Strafverfolgungsbehörden stehen am Anfang künftiger Aktivitäten – sprechen Sie uns gerne direkt an.

Joachim Feist
Gründer und Geschäftsführer der mindUp Web + Intelligence GmbH
Konstanz
E-Mail: autor@pvtweb.de

Herausgeber

Impressum

VERLAG
EMW Exhibition & Media Wehrstedt GmbH
Hagenbreite 9, 06463 Falkenstein/Harz,
OT Ermsleben
Tel.: +49 34743 – 62 090
Fax: +49 34743 – 62 091
Email: info@Wehrstedt.org
Internet: www.Wehrstedt.org
Geschäftsführer: Dr. Uwe Wehrstedt
Amtsgericht Stendal HRB 111856

REDAKTION
Leitender Redakteur und Verleger:
Dr. Uwe Wehrstedt
E-Mail: redaktion@pvtweb.de

REDAKTIONELLE MITARBEIT

pvt Leser:
Ronny Heck
E-Mail: redaktion@pvtweb.de

IuK + Digitalisierung:
Heinz-Dieter Meier
E-Mail: redaktion@pvtweb.de

Wirtschaft & Wissenschaft:
Fabian Lemm
E-Mail: redaktion@pvtweb.de

Waffen und Geräte / Persönliche Ausrüstung:
Michael Waldbrenner
E-Mail: redaktion@pvtweb.de

Kurznachrichten:
Peggy Fleischmann
E-Mail: redaktion@pvtweb.de

Abonnementservice:
Elke Wehrstedt
Tel.: +49 34743 – 62 090
Fax: +49 34743 – 62 091
E-Mail: elke.wehrstedt@wehrstedt.org
Bezugsbedingungen: Erscheint zum 15. eines ungeraden Monats. Bestellung direkt beim Verlag EMW Exhibition & Media Wehrstedt GmbH, s. oben. Die Mindestbezugsdauer beträgt 12 Monate. Kündigungen 3 Monate zum Jahresende. Abonnement ePaper € 25,00 jährlich, Druck Inland: € 45,00 jährlich inkl. Versand; Kombi ePaper + Druck Inland: € 55,00 jährlich inkl. Versand; Druck Ausland: € 52,00 jährlich inkl. Versand; Kombi ePaper + Druck Ausland: € 62,00 inkl. Versand
Bankverbindung: Deutsche Bank,
BLZ 860 700 24, Konto-Nr. 60 30 37 3,
IBAN: DE29 8607 0024 0603 0373 00,
BIC: DEUTDEDBLEG; ISSN 0722-5962

Anzeigenservice:
Fabian Lemm
EMW Exhibition & Media Wehrstedt GmbH
Hagenbreite 9, 06463 Falkenstein/Harz,
OT Ermsleben, Tel.: +49 34743 – 62 090,
Fax: +49 34743 – 62 091
E-Mail: fabian.lemm@wehrstedt.org
Internet: www.Wehrstedt.org
Berechnung der Anzeigen erfolgt unter Zugrundelegung der Preisliste Nr. 42 vom 01.11.2022
Mit Namen oder Initialen gezeichnete Beiträge geben nicht unbedingt die Auffassung der Herausgeber, der Redaktion oder des Verlages wieder. Für amtliche Veröffentlichungen übernimmt die Redaktion keine Haftung. Durch Annahme eines Manuskriptes erwirkt der Verlag auch das Recht zur teilweisen Veröffentlichung, Übersetzung etc. Honorarabrechnung erfolgt grundsätzlich nach Veröffentlichung. Bei allen zur Veröffentlichung bestimmten Zuschriften behält sich die Redaktion das Recht von Kürzungen vor.

Produktion, Umbruch und Layout:
AnKo MedienDesign GmbH, 53340 Meckenheim

www.GPEC.de

GPEC digital

2024

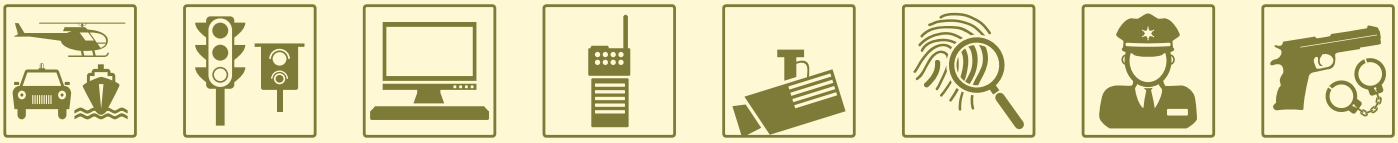
GPEC General Police Equipment Exhibition & Conference®

15. Internationale Fachmesse & Konferenzen für Innere Sicherheit

06. – 08. Mai 2024, Leipziger Messe

Innovationen: Ausrüstung – Ausbildung – Einsatz
Der „Behörden-One-Stop-Event“ für alle Führungsebenen und Sachgebiete.

Die GPEC® ist Europas größte geschlossene Fachmesse für die Polizei und alle Behörden mit Sicherheitsaufgaben – im Jahr 2022 mit 503 Ausstellern aus 32 Staaten und 7.091 Teilnehmern aus 55 Staaten von 5 Kontinenten. Als repräsentativste Gesamtschau aller relevanten Führungs- und Einsatzmittel der Inneren Sicherheit deckt die GPEC® buchstäblich alle Aufgabenbereiche ab. Ein topaktuelles Rahmenprogramm mit Fachtagungen, Seminaren, Trainings und dienstlichen Arbeitskreistreffen macht die GPEC® seit dem Jahr 2000 zum unverzichtbaren Branchen- und Anwenderforum, 2024 als 15. GPEC®-Veranstaltung wieder inklusive der reichweitenstarken GPEC® digital-Thematik. Also seien Sie dabei!



ALLES FÜR DIE INNERE SICHERHEIT

GPEC

GENERAL POLICE EQUIPMENT EXHIBITION & CONFERENCE

GPEC digital

GPEC General Police Equipment Exhibition & Conference®

EMW Exhibition & Media Wehrstedt GmbH
Hagenbreite 9 · 06463 Falkenstein/Harz
E-Mail: info@gpec.de · Internet: www.gpec.de

pvt POLIZEI VERKEHR · TECHNIK

EMW EXHIBITION & MEDIA WEHRSTEDT