Pi-One

Pi-One ist ein junges Unternehmen aus dem Raum Mannheim. Wir bieten unterschiedliche IT-Dienstleistungen in den Bereichen Cyber-Security und IT-Forensik. Neben freien Diensten und Werkzeugen liegt unser Schwerpunkt in den Bereichen:

- Schulung und Beratung im Bereich IT-Sicherheit
- Individuelle Softwarelösungen für kleine bis mittlere Unternehmen
- Schadsoftware und E-Mail Analyse
- Speichermedien- und Rechner-Forensik, auch zur Erstellung von Sachverständigengutachten

Teilhaber

Pi-One wurde Anfang 2009 als Gesellschaft bürgerlichen Rechts (GbR) in Mannheim von

- Dipl. Inf. Markus Engelberth
- Dipl. Inf. Christian Gorecki
- Dr. Jan Gerrit Göbel
- Dr. Philipp Trinius

gegründet. Nach dem Studium an der RWTH-Aachen haben wir an der Universität Mannheim in den Fachbereichen IT-Security und -Forensik gemeinsam geforscht, im Rahmen verschiedener Großprojekte Softwarelösungen für Behörden entwickelt und gerichtsverwertbare forensische Analysen durchgeführt. Auch in der Weiterbildung zu den genannten Themenschwerpunkten verfügen wir über mehrjährige Erfahrung.

Pi-One

Markus Engelberth, Christian Gorecki, Jan Göbel und Philipp Trinius GbR

Berliner Ring 97
64625 Bensheim

Telefon: 06251 / 86 94 03 0

E-Mail: kontakt@pi-one.net

www.pi-one.net

Pi-One

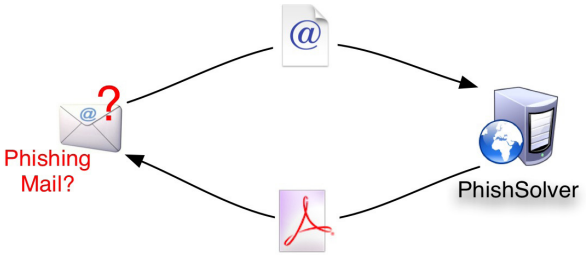
PhishSolver

pi-one.net

Automatische Analyse und Auswertung von Phishing-Mails

Phishing

Phishing-Mails stellen heute eine der größten Bedrohungen im Internet dar. Neben dem großflächigen **Abgreifen von vertraulichen Informationen**, wie z. B. Zugangsdaten zu Bankkonten und E-Mail-Postfächern oder Kreditkarteninformationen, werden Phishing-Mails auch für gezielte Angriffe auf Unternehmen, Regierungen oder einzelne Personen verwendet. Das Erkennen von sogenannten **Targeted Attacks** und das zuverlässige Filtern der hierzu eingesetzten Phishing-Mails ist in der Regel mit sehr hohem Analyseaufwand verbunden.



PhishSolver

Mit PhishSolver stellt Pi-One ein leicht zu verwendendes Analysesystem zur Auswertung von E-Mail-Nachrichten vor. Als **WebService** lässt es sich einfach in Ihre bestehende Infrastruktur integrieren oder kann vollständig losgelöst als externer Dienst (von Pi-One betrieben) genutzt werden.

Die von PhishSolver durchgeführten Analysen beschränken sich nicht auf die Auswertung der Nachricht selbst. Die aus der Nachricht extrahierten Informationen werden zusätzlich mit ausgewählten Datenbanken korreliert, um möglichst umfassende Informationen über die Nachricht zu erhalten. Alle Ergebnisse werden in einem individualisierbaren und leicht verständlichen Bericht zusammengestellt und liegen innerhalb weniger Sekunden vor.

Ergebnis

Das Analyseergebnis übermittelt PhishSolver als übersichtlichen PDF-Bericht direkt an Ihr Postfach. Der Bericht enthält unter anderem

- den genauen **Pfad der Phishing-Mail.** Dieser wird auf einer Weltkarte dargestellt und erlaubt auf einen Blick ein Urteil über Herkunft und Validität der E-Mail-Nachricht.
- die Auflistung der für den Spamversand verwendeten **Benutzerkonten**, zur schnellen Identifizierung bereits kompromittierter Benutzer.
- **Screenshots** der verlinkten Webseiten, die Ihnen einen ersten Eindruck von der Phishing-Kampagne liefern, ohne dass Sie riskieren Ihr eigenes System durch eine Drive-By-Kompromittierung zu infizieren.
- alle relevanten **Kontaktdaten**, um verantwortliche Administratoren oder sonstige technische Ansprechpartner umgehend kontaktieren zu können.

Benutzung

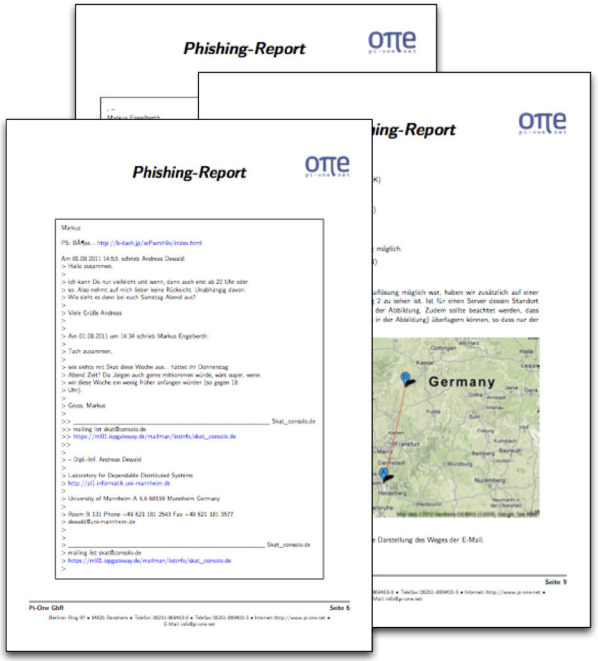
Die Verwendung von PhishSolver ist denkbar einfach. Sie selbst müssen lediglich die **verdächtige E-Mail als Anhang an eine dedizierte E-Mail-Adresse weiterleiten**. Umgehend nach dem Eingang der potentiellen Phishing-Mail wird diese ausgewertet und das Ergebnis innerhalb weniger Sekunden in einem übersichtlichen PDF-Bericht an Sie zurückgeschickt.

Technik

PishSolver besteht aus einer Vielzahl von Analyse- und Auswertungsmodulen. Neben einer Standardauswertung, die allgemeine Informationen umfasst, lassen sich die verschiedenen Module unabhängig konfigurieren, wodurch ein individuell angepasster Bericht ermöglicht wird. Auf diese Weise erscheinen Informationen, die Sie als weniger relevant einstufen, gar nicht erst in dem Bericht, wodurch Übersichtlichkeit garantiert ist.

Datenschutz

Die Möglichkeit verschiedene Analysemethoden getrennt voneinander zu konfigurieren erlaubt es **besonderen Datenschutzanforderungen** gerecht zu werden. Gezielte Phishing-Angriffe enthalten oft vertrauliche Informationen, die Angreifer vorab recherchiert haben, um die Phishing-Mail zu personalisieren. Um derartige Informationen zu schützen, werden alle Analysemodule in **aktive** und **passive** unterschieden: Während aktive Module weitere Informationen von ausgewählten Datenquellen abrufen, arbeiten passive Module ausschließlich lokal. Durch eine Einschränkung auf passive Module kann somit die Vertraulichkeit von Informationen gewährleistet werden.



Systemintegration

Auf Grund der klaren Schnittstelle kann PhishSolver nicht nur als **unabhängiger Dienst** genutzt werden, sondern auch in existierende IT-Infrastrukturen problemlos integriert werden. Insbesondere zur **Erweiterung existierender Sicherheitslösungen** bietet PhishSolver eine optimale Ergänzung, um verdächtige E-Mails innerhalb von nur wenigen Sekunden zu analysieren.

Für weitere Informationen besuchen Sie uns unter **http://www.pi-one.net.**