THE PENTEST EXPERTS.

In diesem Newsletter erwarten Sie folgende Inhalte:

Sehr geehrte Kunden,
liebe Geschäftspartner,
Freunde und Bekannte,

die meisten Firmen haben ihre eigene faszinierende Geschichte. Einige Unternehmen entspringen einer Idee und des grenzenlosen Optimismus sowie der unverbrüchlichen Tatkraft ihrer Gründer. Mancher erfolgreiche Konzern, wie beispielsweise einige IT-Firmen im Silicon Valley, hat seine Wurzeln in einer zu einer Bastelwerkstatt umgebauten Garage. Die Geschichte der SySS GmbH jedoch geht zurück auf ein Weihnachtsgeschenk. Am 24.12.1983 entdeckte ich unter dem Weihnachtsbaum meiner Familie ein Geschenk, das mein Leben entscheidend prägte: einen nagelneuen Commodore C64[1]. Dieser motivierte mich, ihn bis ins Detail kennenzulernen und voller Begeisterung begann ich, ihn zu programmieren und alles daran zu setzen, ihn selbst in Grenzbereichen zu meistern. Im Jahr 1983 gab es natürlich noch kein Internet. Es machte mir Spaß, Computerspiele so zu manipulieren, dass ich die von Drachen bedrohte Prinzessin in jedem Fall retten konnte, oder den Highscore mancher Spiele etwas zu frisieren. Ebenso interessierte ich mich dafür, Kopierschutzmechanismen zu knacken und eigene Programme zu schreiben. 15 Jahre später, im Sommer 1998, gründete ich während meines Informatikstudiums die Firma SySS und machte meine Leidenschaft zum Beruf. Durch einen originellen Zufall wurden gleich am Tag der Anmeldung meines Gewerbes die Firmen HP und IBM meine ersten Kunden.

Dieses Jahr feiert SySS 15-jähriges Bestehen. Dies ist für mich ein passender Anlass, mich bei meinen wichtigsten Wegbegleitern zu bedanken, nämlich bei meinen Mitarbeitern. Sie sind das Wertvollste, das ich habe, und bilden ein starkes Team, das unermüdlich nach neuen Angriffswegen sucht, unsere Kunden bei der Identifikation von Schwachstellen unterstützt, meine Firma auf allen Ebenen (vor allem technisch und administrativ) am Laufen hält und mir in vielen Angelegenheiten mit Rat und Tat zur Seite steht. Jeder einzelne Mitarbeiter ist wichtig an seinem Platz und auf jeden bin ich stolz!

Angesichts unseres Jubiläums frage ich mich, wie die SySS GmbH wohl in weiteren 15 Jahren aussehen wird. Für mich steht fest, dass auch dann Penetrationstests und Incident Response zu unseren Kerntätigkeiten zählen werden. Ebenso bin ich überzeugt davon, dass ich weiterhin Geschäftsführer und Gesellschafter sein werde. Welche Technologien wir dann allerdings verwenden und wie wir in 15 Jahren Penetrationstests durchführen werden, ist absolut offen. Eines ist sicher, die SySS GmbH wird am Ball bleiben und gewiss vorne mit dabei sein.

Herzliche Grüße,
Ihr Sebastian Schreiber

Aktuelle Events

27.11.13	„Spionage 2.0 – Wirtschaftsschutz neu denken“ Podiumsdiskussion mit Sebastian Schreiber
27.11.13	LH[1] IHK, Chemnitz
11.12.13	LH[1] IHK BIEG, Frankfurt/Main

[1] Live Hacking

Vorankündigung:
Die SySS GmbH wird bei der CeBIT 2014, vom 10.03. - 14.03.14 in Hannover, präsent sein.

Detaillierte Informationen zu diesen Veranstaltungen finden Sie auf unserer Homepage www.syss.de.

Aktuelle Schulungen

Mobile Device:
05. - 06.03.14

IT-Security I:
17. - 18.03.14
12. - 13.05.14

IT-Security II:
19. - 20.03.14
14. - 15.05.14

WLAN:
25. - 26.03.14

IPv6:
28.03.14

Windows-Angriffe:
02. - 03.04.14
27. - 28.05.14

Exploits:
09. - 10.04.14

VoIP
29. - 30.04.14

IT-Forensik:
06. - 08.05.14

Incident Response:
20. - 22.05.14

Web-App
03. - 04.06.14

PenTests:
06.06.14

IT-Recht:
27.06.14

Bei Teilnahmewunsch oder Fragen wenden Sie sich bitte an info@syss.de.

Sollten Sie den Newsletter nicht beziehen wollen, dann teilen Sie uns dies bitte unter newsletter@syss.de mit, wir werden Sie dann umgehend aus dem Verteiler entfernen.

[1] Der technische Fortschritt ist rasant:
Ein C64 hatte damals insgesamt 64KB Speicher und eine Auflösung von 320x200 Pixel. Im Vergleich dazu ist ein iPhone winzig klein, hat aber eine 11 mal höhere Auflösung. Wenn ich die Daten, die ich auf einem iPhone gespeichert habe, auf eine Reihe C64er verteilen wollte, würde ich hierzu sämtliche in Deutschland verkauften Exemplare (ca. 1 Mio Stück) benötigen.

Impressum:
SySS GmbH · Wohlboldstraße 8 · 72072 Tübingen · Tel. +49 (0)7071 407856-0 · E-Mail: info@syss.de · http://www.syss.de · Geschäftsführer: Diplom-Inform. Sebastian Schreiber
Verantwortlich für Inhalt: Marcus Bauer

THE PENTEST EXPERTS.

Panta Rhei – Alles fließt!

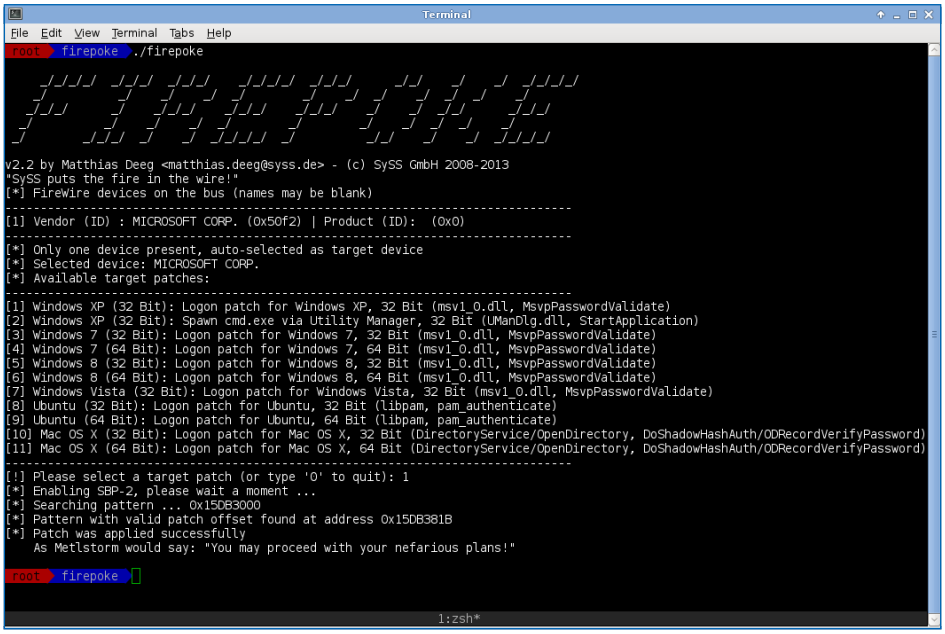
Über die „Research & Development"-Abteilung bei der SySS GmbH – von Matthias Deeg

Panta rhei! Alles fließt! – Oder: Nichts ist so beständig wie der Wandel. Diese Erkenntnis hatten schon die alten Griechen – genauer gesagt Heraklit – und nie zuvor war diese Einsicht besser nachzuvollziehen als in der heutigen Zeit, in der es zunehmend schwerer fällt, mit dem Fortschritt Schritt zu halten. Besonders im Bereich Informationstechnik ist diese Entwicklung gut zu beobachten, wo sich Produktzyklen in den vergangenen Jahren immer weiter verkürzt haben. Soft-, Firm- oder Hardware ist teilweise bereits zum Verkaufsstart nicht mehr aktuell und es liegen entsprechende Updates beziehungsweise neue Produktversionen vor, die Fehler beheben oder neue Funktionen bereitstellen.

Wir, die IT-Sicherheitsberater bei der SySS GmbH, fühlen uns dazu verpflichtet, mit dem rasanten Tempo dieses Fortschritts mitzuhalten und im wahrsten Sinne des Wortes über den aktuellen Stand der Technik in unserem Tätigkeitsfeld, der Informationssicherheit, bestens informiert zu sein. Unsere eigenen Aktivitäten in diesem Bereich bauen wir seit Jahren kontinuierlich aus und haben im Zuge dieses Prozesses zu Beginn diesen Jahres eine eigene Forschungs- und Entwicklungsabteilung (R&D, Research & Development) ins Leben gerufen, die für uns und unsere Kunden interessante Forschungs- und Entwicklungsprojekte auf verbesserte Weise planen, koordinieren und durchführen kann als zuvor.

Im Rahmen solcher Projekte haben unsere Mitarbeiter die Möglichkeit, neue Erkenntnisse in für sie spannenden Bereichen der Informationssicherheit zu interessanten Themen zu gewinnen, Lösungen zu offenen Problemen zu finden und diese praxistauglich umzusetzen. Ein Themengebiet, mit dem wir uns beispielsweise regelmäßig beschäftigen, ist die Kryptografie. Kryptografische Verfahren beziehungsweise deren Implementierung spielen insbesondere für den Schutz der Vertraulichkeit und Integrität von elektronischen Daten eine zentrale Rolle und finden in zahlreichen Technologien, Protokollen und Hard- wie auch Softwareprodukten Anwendung. Unsere Forschungs- und Entwicklungsprojekte sind kein reiner Selbstzweck, sondern sie haben neben dem Erkenntnisgewinn primär das Ziel, unsere alltägliche Arbeit im Bereich Sicherheitstests von informationstechnischen Systemen zu verbessern.

Die Entwicklung von neuen beziehungsweise die Pflege von bereits existierenden In-House-Software-Tools spielt dabei eine wichtige Rolle. Software-Tools wie FirePeek/FirePoke für Speicheranalysen und -manipulationen über die IEEE-1394-Schnittstelle (FireWire) und der Portscanner Wolpertinger werden zum Beispiel seit mehreren Jahren erfolgreich bei Penetrationstests eingesetzt und stetig weiterentwickelt, um neuen Anforderungen gerecht zu werden. Die Weiterentwicklung von Software-Tools kann dabei auf Anforderungen beruhen, die funktionaler Natur sind, wie etwa die Unterstützung eines neuen Betriebssystems, oder die nicht-funktionalen Charakter haben, wie zum Beispiel eine Verbesserung der Benutzbarkeit oder Zuverlässigkeit. Darüber hinaus entstehen immer wieder neue Software-Tools, wie diverse automatisierte Scanner, die bestimmte Sicherheitsüberprüfungen im Rahmen von Penetrationstests enorm vereinfachen, wie beispielsweise ADScan (Active Directory Scanner), TYPO3-Scanner, wfss (Windows File System Scanner) und wrs (Windows Registry Scanner). Diese Werkzeuge dienen dem Zweck, unsere Arbeit als IT-Sicherheitsberater effizienter und effektiver zu machen.



Screenshot FirePoke, Quelle: SySS

THE PENTEST EXPERTS.

Auch bei vielen Forschungsprojekten entstehen neue Werkzeuge, Code-Schnipsel oder Skripte, die nicht nur bei Live-Hacking-Demonstrationen und Publikationen Verwendung finden, um unserem Publikum und dem Leser zu zeigen, wie manche Angriffe durchgeführt werden können, sondern auch bei der Durchführung von Sicherheitstests. Bei Forschungsaktivitäten zu den Themen „Android-Trojaner", „Antivirus Evasion (Umgehen von Antivirensoftware), „NFC-Kreditkarte" und „Windows PowerShell" sind in diesem Jahr mehrere nützliche Software-Tools entstanden. Ein Beispiel hierfür ist der zu Demonstrationszwecken entwickelte Android-Trojaner SPAT (SySS PoC Android Trojan), der bereits in zahlreichen unserer Live-Hacks und auch in mehreren Fernsehauftritten eingesetzt wurde, um die Gefahren und die technischen Möglichkeiten von Schadsoftware in Form sogenannter „Trojaner" (eigentlich „Trojanischen Pferden") anschaulich zu zeigen, wie etwa das Erstellen von Bewegungsprofilen, das Abhören von Telefongesprächen oder der Zugriff auf persönliche Daten.

Ein weiteres nützliches Software-Tool ist die Build-Umgebung ShCoLo (Shellcode Loader) für das Umgehen von Schutzmaßnahmen von Endpoint-Protection-Lösungen bei Penetrationstests, unter anderem für die Durchführung zielgerichteter Angriffe (Targeted Attacks), die etwa über den Angriffsvektor E-Mail gegen ausgesuchte Zielpersonen unternommen werden. Im Rahmen von Forschungsprojekten finden wir auch immer wieder neue Sicherheitsprobleme in IT-Produkten, mit denen wir gemäß unserer SySS Responsible Disclosure Policy verantwortungsvoll umgehen. Bisweilen kommt es auch vor, dass wir in Forschungsprojekten Ergebnisse erzielen, die auf das konkrete Projekt bezogen als Fehlschlag bewertet werden müssen, aber die sich in einem ganz anderen Kontext als sehr nützlich erweisen – vergleichbar mit der Geschichte von Entdeckungen und Erfindungen mit weitaus größerer Tragweite, wie Penicillin, Teflon oder Gummireifen.

Das Hauptaugenmerk unserer Forschungs- und Entwicklungstätigkeit in diesem Jahr lag auf verschiedenen Entwicklungsprojekten. Auch im kommenden Jahr wird die Entwicklung und Pflege von Software-Tools einen wichtigen Platz einnehmen. Für 2014 ist jedoch das erklärte Ziel, mehr Zeit für Forschungsaktivitäten aufzuwenden und sich verstärkt Themen zu widmen, denen in der Vergangenheit weniger Aufmerksamkeit zuteil wurde. Konkrete Beispiele für derartige Forschungsprojekte sind die beiden Themenkomplexe Codeanalyse-Methoden und Fuzzing-Techniken, wo wir noch Potenzial sehen, unsere Kompetenzen hinsichtlich Sicherheitsanalysen von Softwareprodukten (sowohl open- als auch closed-source) zu verbessern. An guten Ideen für Forschungs- und Entwicklungsprojekte mangelt es uns nicht und wir streben auch in Zukunft danach, den besten dieser Ideen nachzugehen. Denn eines ist sicher, die Welt ist in stetigem Wandel und wir teilen das Bewusstsein Heraklits, der sagte „Wer in dieselben Flüsse hinabsteigt, dem strömt stets anderes Wasser zu." Und so hoffen wir, die IT-Welt durch unsere Arbeit ein kleines bisschen sicherer zu machen.