atsec the information security provider

NEWS 12/09

Sehr geehrte Damen und Herren,

wir freuen uns, Ihnen mit dem Newsletter für das 4. Quartal 2009 unsere neue Website vorstellen zu können. Wir haben uns für ein anderes Design entschieden, aber die Navigationsstruktur ist im Wesentlichen unverändert geblieben und Ihnen vertraut. Unser Angebot an Informationen ist an vielen Stellen ergänzt und für Sie zugänglicher gemacht worden. Die Übersicht über unsere Services wurde grundsätzlich überarbeitet.

„Der triumphale Fortschritt der Wissenschaften macht tiefgreifende Veränderungen für die Menschheit unabwendbar."

(Manifest der futuristischen Malerei, 1910)

Die Inspiration für das Design der neuen atsec Website, das sich auch in unserem aktuellen Newsletter widerspiegelt, entstammt dem Futurismus, der avantgardistischen Kunstbewegung des frühen zwanzigsten Jahrhunderts, die der Faszination von Geschwindigkeit, Technologie und Wissenschaft ergeben war. Die Kunst dieser Zeit rückt Licht und Dynamik ins Zentrum und konzentriert sich auf die reine Darstellung von Bewegungsabläufen. Formen und Linien fließen dabei ineinander, um Kontinuität darzustellen. Die futuristische Kunst ist nicht nur farbenfroh und ästhetisch gefällig, sondern auch dynamisch, kreativ und zukunftsweisend.

Eben diese Eigenschaften zeichnen auch atsec aus. Wir sind führend auf dem Gebiet der Informationssicherheit. Diese Position haben wir erreicht, durch den Aufbau eines Gefüges von Standards und Methodiken, das sich auf die Sicherheitsanforderungen unserer Kunden konzentriert und eine solide Basis für die gesamte Branche bietet.

Wir sind uns bewusst, dass unsere Führungsposition nur dann von Dauer ist, wenn wir weiterhin maßgebliche Lösungen realer Probleme anbieten können. Wir müssen dynamisch sein und neue Aufgabenstellungen vorhersehen, statt in vergangenen Erfolgen zu verharren. Wir müssen progressiv denken, um den zukünftigen Bedarf an Informationssicherheit identifizieren zu können. Und nicht zuletzt ist unsere Kreativität gefragt, um eine erfolgreiche Strategie und passende Lösungen zu planen und damit unsere Führungsposition auf dem Gebiet der Informationssicherheit zu erhalten.

Ich wünsche Ihnen und Ihren Familien ein besinnliches Weihnachtsfest und ein glückliches, erfolgreiches Jahr 2010.

Salvatore la Pietra
CEO

Falls Sie den atsec Newsletter in Zukunft nicht mehr erhalten möchten, senden Sie bitte eine E-Mail mit dem Betreff „unsubscribe" an newsletter@atsec.com.

atsec auf der 10. ICCC

Die Fachkenntnis unserer Mitarbeiterinnen und Mitarbeiter ist sehr gefragt: Sie gehören internationalen Kommissionen an, halten Vorträge auf Konferenzen und schreiben Bücher und Fachartikel.

Auf der 10. ICCC in Tromsø, Norwegen war atsec gleich mit fünf Vorträgen vertreten:

- Evidence based Evaluations Chances and Challenges (Helmut Kurth)
- Trusting Virtual Trust (Jeremy Powell)
- Taking White Hats to the Laundry: How to Strengthen Testing in CC (Apostol Vassilev)
- An Attack Surface based Approach to Evaluation (Helmuth Kurth)
- OSPP: A Flexible Approach to Operating Systems Security (Gerald Krummeck)

Ken Hake, Laboratory Manager für atsec U.S., kommentierte: „Mehrere Redner auf einer Veranstaltung wie der ICCC stellen zu können, zeigt deutlich unser ständiges Engagement, die Common Criteria weiter zu entwickeln und macht gleichzeitig unseren Anspruch deutlich zur Community von IT Security Profis beizutragen, die diesen Standard für ihre tägliche Arbeit nutzen."

Brave New World 2.0

Die schöne neue Welt des Web 2.0 eignet sich nicht nur für neuartige Anwendungen, sondern bietet Hackern eine Vielzahl lohnender Ziele.
Viele Unternehmen haben mittlerweile Prozesse implementiert, um regelmäßig und automatisiert Sicherheits-Patches für Betriebssysteme und Anwendungssoftware zu installieren. Gleichzeitig wenden sich Angreifer verstärkt den „neuen“ Anwendungen im Internet zu (Web-Shops, Bezahlsysteme, soziale Netzwerke), versprechen diese doch einerseits lohnende Informationen wie Kreditkartendaten und andererseits Anonymität durch gestohlene Zugangsdaten für betrügerische Handlungen. Da diese Anwendungen z. T. erheblich individuell angepasst und erweitert werden, lassen sich allerlei Schwachstellen in diesen Erweiterungen finden, die nicht autorisierten Zugriff erlauben.

Die bisher üblichen Überprüfungen von Systemen mittels Penetrationstests verfehlen ihre Wirkung bei dieser neuen Art von Angriffen, da sie lediglich auf das Betriebssystem und Standard-Anwendungen wie Web Server abzielen.

Web Application Pentesting ist eine Weiterentwicklung dieser klassischen Penetrationstests: Der Pentester untersucht gezielt individuelle Systeme der Kunden, um spezifische Schwachstellen offen zu legen und als Basis für weitere Attacken gegen das Netzwerk zu nutzen.

Eine oft unterschätzte Schwachstelle ist der Mensch – also der Benutzer einer Applikation, als Kunde ebenso wie als Angestellter eines Unternehmens. Die Komplexität von Systemen zusammen mit oft unübersichtlichen Abläufen bietet eine ideale Basis für „social engineering“ Angriffe. Hierbei werden per E-Mail, Telefon oder über manipulierte Webseiten vertrauliche Informationen abgegriffen, ohne dass sich der Angegriffene dessen überhaupt bewusst ist. Häufigste Beispiele hierfür sind sogenannte „Phishing“-Angriffe, bei denen z. B. TANs für Online-Banking gesammelt werden, sowie Trojaner, also kleine Programme, die auf dem PC des Opfers sämtliche Eingaben mitprotokollieren und die Festplatte nach gespeicherten Passwörtern durchsuchen, übertragen werden.

Die Vorgehensweise unserer Pentester imitiert die der Hacker:

- Als erstes werden Informationen über das Ziel gesammelt, also Systeme, verwendete Software, Personen, E-Mail Adressen, gängiger Firmen-Jargon. Diese Informationen sind nicht nur durch direkte Scans der Systeme erhältlich, sondern ebenso über verschiedenste Quellen im Internet, in denen bspw. Mitarbeiter über technische Probleme diskutieren.
- Anhand dieser Informationen wird der „Entry Point“ ausgewählt, also die Stelle, an der ein Eindringen am einfachsten erscheint.
- Der Pentester versucht als nächstes, sich über Social Engineering Zugang zu Systemen im Unternehmensnetzwerk zu verschaffen
- So erübrigt sich immer öfter ein klassischer Angriff, z. B. das systematische Ausprobieren von häufig verwendeten Passwörtern. Die unmittelbare Folge hiervon ist, dass das unerlaubte Eindringen nicht mehr bemerkt wird – das betroffene System sieht oft nur noch legitim aussehende Zugriffe.
- Sobald ein erster Zugang existiert, werden „von innen“ weitere Systeme geprüft und Schwachstellen analysiert.

War Games

Bemerkung: Namen und Gegebenheiten wurden aus Gründen der Anonymität verändert. Alle Ähnlichkeiten zu realen Unternehmen und Personen sind rein zufällig.

Ein größerer Finanzdienstleister beauftragte atsec, einen Penetrationstest gegen einen Teil seiner Serversysteme (mehrere Mail- und Webserver) und Gateways (mehrere Firewalls und VPN Gateways) durchzuführen. Der Test sollte laut Vereinbarung auf konventionelle Art und Weise stattfinden. Unser Pentester sammelte Informationen über Netz-

werke, Hosts, Netzwerkdienste und verwendete Serversoftware. Es wurde versucht, Firewalls zu umgehen und bekannte Schwachstellen in der Serversoftware auszunutzen, jedoch ohne Erfolg. Unser Auftraggeber war sehr zufrieden damit, dass die eingebauten Systeme scheinbar alle Angriffe erfolgreich abwehren konnten.

Da wir für den Test noch einen Tag Reserve hatten, schlugen wir dem Kunden vor, seine Netzwerksicherheit auch gegen die neueren Arten von gezielten Angriffen und Industriespionage prüfen zu lassen. Der Finanzdienstleister genehmigte uns daraufhin zusätzlich „social engineering“ Angriffe, von denen die Mitarbeiter nicht vorab in Kenntnis gesetzt wurden.

Unser Pentester begann damit, zusätzliche Informationen aus öffentlichen Internetquellen zu sammeln und für einen gezielten Angriff zu korrelieren. Die Ausbeute dieser Informationsgewinnung waren ca. 100 gültige E-Mail Adressen von Mitarbeitern des Finanzdienstleisters, diverse Forums- und Weblog Posts der firmeninternen IT-Abteilung und viele weitere interessante Details über Mitarbeiter und das Unternehmen.

Der Plan unseres Testers war, Mitarbeiter des Unternehmens auf eine von ihm präparierte Webseite zu locken, die beim Aufruf verschiedene Schwachstellen im Browser des Mitarbeiters und dessen installierter Software ausnutzt, um ein Trojanisches Pferd zu installieren. Somit hätte unser Pentester die volle Kontrolle über den Opfer-PC.

Also sendeten wir authentisch aussehende E-Mails, die sogar direkt vom E-Mail Server des Finanzdienstleisters stammten, an die 100 Mitarbeiter E-Mail Adressen und hofften darauf, dass die Mitarbeiter den „Phish” fangen würden. Eine E-Mail, die vom hauseigenen IT-Support stammte und höflich darum bat, eine Internetadresse aufzurufen, schien für die meisten Mitarbeiter keine Gefahr darzustellen. Innerhalb von circa einer Stunde bekam unser Tester ca. 20 Kontrollverbindungen zu den Mitarbeiter-PCs, auf denen das Trojanische Pferd erfolgreich installiert wurde. Aufgrund der hohen Erfolgsquote riefen wir unseren äußerst überraschten Kunden sofort an und beschlossen, den Test abzubrechen, da das erfolgreiche Eindringen in das Netzwerk ja schon bewiesen wurde und weitere Angriffe die Leistung des Netzwerks u. U. beeinträchtigt hätten.

Ein echter Angreifer hätte an dieser Stelle sicherlich unbemerkt alle sensiblen E-Mails und Dokumente auf den einzelnen Rechnern stehlen können und Tastaturanschläge aufgezeichnet. Von hier wäre er dann in Datenbanken, Verwaltungssoftware und das Netzwerk eingedrungen und hätte Informationen gestohlen, gelöscht und manipuliert. Oftmals werden solche PCs, nachdem sie infiziert wurden, in ein Netzwerk aus „Zombie“-PCs eingegliedert, die zu einem sog. Bot-Netz zusammengeschlossen sind und einem „Bot Master“ dazu dienen, weitere Netzwerke anzugreifen, was manchmal auch rechtliche Konsequenzen für die Besitzer der Zombie PCs (das Unternehmen selbst) haben kann.

Information Warfare

Hacker haben sich gut gerüstet für eine neue Art der digitalen Kriegsführung, in der das Individuum mehr und mehr zum direkten Ziel des Angriffs wurde. Ein Individuum, welches immer bereitwilliger seine Gedanken, die eigene Privatsphäre und jeden Schritt und Tritt einer breiten Öffentlichkeit mitteilt. In einer Welt, die sich abhängig gemacht hat von einem von Menschen erschaffenen Web 2.0, einem Dschungel aus Links, Blogs, Tag-Clouds und digitalen Identitäten, in der man nur noch über Twitter, Facebook und E-Mails kommuniziert, ist alles miteinander verbunden und Hacker wissen, welchen Spuren sie in diesem Dschungel folgen müssen, um ihre Opfer in die sichere Falle locken zu können.

Weitere Artikel und die erwähnten Vorträge finden Sie unter: http://atsec.com/us/publications-white-papers.html

Vier atsec-Kunden erhalten Common Criteria Zertifikat auf der 10. ICCC

Wir freuen uns, die Vergabe von Common-Criteria-Zertifikaten an vier unserer Kunden bekannt zu geben. Die Zertifikate wurden während der 10. International Common Criteria Conference in Tromsø, Norwegen überreicht.

Es erhielten Zertifikate:

- IBM für IBM z/OS Version 1 Release 10
- Oracle für Oracle Database 11g Enterprise Edition, Release 11.1.0.7 with Oracle Label Security
- Microsoft für Microsoft Windows Server 2008 Hyper-V Role with HotFix KB950050

Diese Produkte wurden von atsec information security nach EAL 4+ – der höchsten Prüfstufe, die komplexe, kommerzielle Produkte mit vertretbarem Aufwand erreichen können – evaluiert.

Des Weiteren hat IEEE mit Hilfe von atsec information security die Validierung eines neuartigen Schutzprofils für Drucker abgeschlossen: IEEE 2600™, „STANDARD FOR INFORMATION TECHNOLOGY: HARDCOPY SYSTEM AND DEVICE SECURITY“.

Gerald Krummeck, Common Criteria Prüfstellenleiter für atsec, bemerkte dazu: „Einerseits zeigen diese Erfolge atsecs Führungsposition im Bereich der IT-Sicherheit, andererseits ist die Evaluierung von komplexen IT-Produkten auch ein wichtiger Test für die Common Criteria selbst. Wieder einmal zeigt sich, wie gut sich der CC-Standard auf eine Vielzahl von sehr unterschiedlichen Technologien von hoher Komplexität anwenden lässt.“

Der erfolgreiche Abschluss dieser Projekte ist ein weiterer Beweis für atsecs Kompetenz, wenn es um die Evaluierung komplexer Systeme auf hohem Sicherheitsniveau geht.

Übergabe der CC-Zertifikate in Tromsø

atsec präsentiert „Secure Network Zones-Vortrag“ auf der ISSE 2009

Mehr als 350 Teilnehmer diskutierten auf der ISSE (Information Security Solutions Europe) in Den Haag aktuelle IT-Sicherheitsthemen. Europäische und internationale Experten aus Forschung und Wirtschaft stellten IT-Sicherheitsszenarien, Studienergebnisse und Verfahren zu Identity Management, Datenschutz und Social Engineering sowie Cloud Computing vor. Peter Wimmer, Geschäftsstellenleiter von atsec München, präsentierte seinen Vortrag zum Thema „Secure Network Zones“.

Der Vortrag beschreibt die Implementierung von sicheren Netzwerkzonen einschließlich der Einstufung von Daten, der Zuweisung von Anwendungen zu bestimmten Zonen und der Kontrolle des Datenflusses. Darüber hinaus wird eine Möglichkeit für die Migration von existierenden Umgebungen aufgezeigt und für spezielle Anwendungsfälle werden Empfehlungen gegeben.

Erfolg für atsec in Penetrationstest-Wettbewerb

Sascha Herzog, Berater für atsec, nahm im Oktober an einem Hacking-Workshop und -Wettbewerb auf der „Attack and Defense“-Konferenz teil. Er belegte den zweiten Platz in einem Feld von 50 Mitbewerbern.

Herzogs Erfolg verdeutlicht atsecs Erfahrung und Kompetenz, wenn es um Penetrationstests und die Sicherheit von Web-Anwendungen geht. Weitere Themen der Workshops waren Windows- und Linux-Sicherheit, Web-Anwendungs-Sicherheit (z. B. SQL-Injection, das Umgehen der Authorisierung, Cross-Site-Scripting, Sicherheitsrisiken durch Firefox-Plugins), Netzwerksicherheit und andere aktuelle Inhalte zum Thema Penetrationstests.

Gerald Krummeck, Chief Operating Officer für atsec Germany, sagte dazu: „Wir sind stolz auf Saschas eindrucksvollen Beweis für atsecs weitreichende Erfahrung mit Sicherheitstests. Diese Tests werden immer wichtiger für unsere Kunden, die web-basierende Dienstleistungen und Produkte anbieten. Unsere Herangehensweise ermöglicht es uns nicht nur Schwachstellen zu finden, sondern auch strukturierte, auf IT-Sicherheitsstandards basierende Lösungen zu implementieren, die verhindern, dass diese Sicherheitslücken in der Zukunft noch einmal zu einem Problem werden.”

Unsere Berater sprechen häufig auf Konferenzen und veröffentlichen zahlreiche Artikel und Whitepapers. Einige unserer Mitarbeiter sind außerdem in internationalen IT-Sicherheits-Gremien tätig.

IMPRESSUM

atsec information security GmbH
Steinstr. 70
81667 München
Deutschland
Telefon: +49-89-442-49-830
Telefax: +49-89-442-49-831
E-Mail: info@atsec.com

Vertretungsberechtigte Geschäftsführer:
Salvatore la Pietra
Staffan Persson
Registernummer: HRB 129439
Registergericht: Amtsgericht München
UST-ID-Nr. gemäß § 27a UStG: DE205370914
Verantwortlich für den Inhalt:
Gerald Krummeck (Anschrift s.o.)