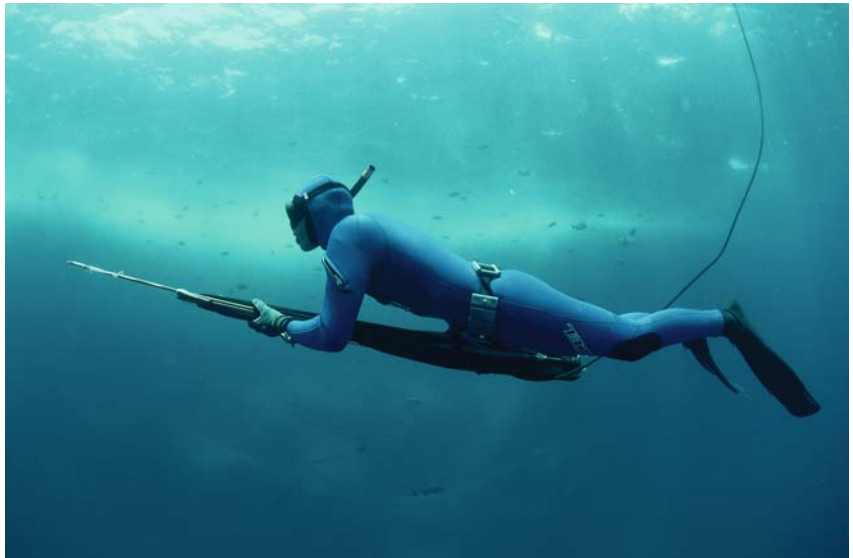


IT-Security Trends unter der Lupe

Von Zeit zu Zeit ist es angebracht, prognostizierte Security-Trends kritisch zu betrachten. Eine der Prognosen, die sich erfüllt hat, ist der Schwenk von wahllos verbreiteten Schädigungen hin zu gezielten Attacken. Egotäter werden von Gruppen mit finanziellem Interesse abgelöst. Wir greifen hier exemplarisch die Entwicklungen im Spezialbereich Phishing auf – und zeigen, wie sich Schutzmaßnahmen an der neuen Situation orientieren können.



Phishing ist eine der Bedrohungen, die definitiv zunimmt. Das Gefährliche am Phishing ist neben den bisher bekannten Schäden, wie z.B. Missbrauch von Benutzernamen und Passwörtern für illegale Transaktionen, dass die tatsächlichen Möglichkeiten des „Phishers“ unterschätzt werden. Gezieltes Phishing liefert dem Angreifer genügend Informationen, um auch Unternehmensnetze angreifen zu können. Bekannt ist, dass seit über einem Jahr Internet-Nutzer mit immer größeren Wellen von Phishing-Mails konfrontiert werden. In den Anfängen waren die e-Mail Köder oft noch unprofessionell gestaltet. Das gleiche galt für die Seiten der URLs, auf denen die Benutzer ihre Daten abgeben sollten. Trotzdem wurde der Bedrohung durch Phishing bereits damals eine wachsende Bedeutung vorausge-

Beim Phishing geht der Trend zum Spear-Phishing: Die Angriffe werden gezielter und sind von kommerziellem Interesse motiviert.

sagt, vor allem im Bereich des Finanzwesens. Diese Prognose hat sich nach unseren Erfahrungen leider voll und ganz erfüllt.

Attacken werden kommerziell

Phishing wird heute professioneller als je zuvor betrieben. Die e-Mail Köder sind glaubwürdig aufgesetzt, die korrespondierenden Webseiten sind von Originalseiten kaum mehr zu unterscheiden. Und auch die Voraussage, dass Phishing vor allem im Finanzbereich wichtig werden wird, ist voll eingetreten. Banken sind fast täglich damit konfrontiert, dass ihre Kunden via Phishing zur Preisgabe

Einladung zum Bacher Systems Breakfast 7. September 2006

Mehr über **aktuelle Entwicklungen im IT-Security Bereich** erfahren Sie auf dem nächsten Bacher Systems Breakfast am 7. September 2006 (9:30 bis 11:00) im Atelier Augarten.

Wir betrachten sieben IT-Security Trends unter einer kritischen Lupe und berichten aus unseren Erfahrungen. Sie erfahren, welche Lösungsansätze in der Praxis am sinnvollsten sind.

Die Teilnahme ist kostenlos, um rechtzeitige Anmeldung unter www.bacher.at/breakfast wird gebeten.



Newsletter 5/2006

Informationen für IT-Sicherheit und IT-Infrastruktur

von Zugangsinformationen geködert werden. Wobei erwähnt werden muss, dass dieses Beispiel noch eine der harmloseren Anwendungen von Phishing ist. Viel gefährlicher sind die neuen Spear-Phishing Attacken, die sich zielgerichtet gegen die Mitarbeiter eines bestimmten Unternehmens richten. Beispielsweise wird den Benutzern eine Mitteilung des Administrators vorgegaukelt. Auf diese Weise werden Zugangsinformationen zu e-Mail Accounts und Webapplikationen erschlichen. Die Entwicklung Richtung Spear-Phishing lässt nur einen Schluss zu: Hinter Phishing stecken nicht mehr die subversiven Aktivitäten Einzelner, sondern massive kommerzielle Interessen. Eine ähnliche Tendenz ist im gesamten IT-Security Bereich zu finden. Attacken, die den persönlichen Ehrgeiz von Einzeltätern befriedigen sollen, nehmen ab, gezielte Angriffe durch gut organisierte Gruppen nehmen zu. Bestätigt werden unsere Beobachtungen auch immer wieder in Gesprächen mit unseren Auftraggebern. Phishing wird mittlerweile als ernste Bedrohung wahrgenommen. Nicht nur wegen der zunehmenden Professionalität in der Umsetzung, sondern auch deshalb, weil laut IT-Security Herstellern bis zu 5% der geköderten Benutzer bei einer Phishing-Attacke tatsächlich reagieren. Die Bedrohung hat sich also in der prognostizierten Art und Weise entwickelt. Wir werden immer wieder darauf angesprochen, ob wirksame Schutzmaßnahmen verfügbar sind.

Schutz gegen Spear-Phishing

Wird gegen ein Unternehmen eine gezielte Spear-Phishing Attacke geführt, so werden – je nach Unternehmensgröße – oft hunderte oder gar tausende Mitarbeiter geködert. Wenn man die hohen Response-Raten von bis zu 5% in Betracht zieht, lässt sich leicht ausrechnen, dass die Erfolgsaussichten eines solchen Angriffs sehr hoch sind. Innerhalb kurzer Zeit stehen einer organisierten Gruppe mindestens dutzende Zugriffsmöglichkeiten auf Webportale des Unternehmens zur Verfügung. Da diese Gruppen von finanziellem Interesse getrieben sind, kann der Schaden immens sein.

Gegen Angriffsmuster via Phishing hilft nur eine Doppelstrategie: Einerseits die Bewusstseinsbildung bei den eigenen Mitarbeitern, andererseits der Aufbau gezielter technischer Schutzmaßnahmen:

- Der Einsatz eines e-Mail Filters ermöglicht es, einen Großteil der Phishing-Köder von den Mitarbeitern fernzuhalten. Eingehende e-Mails werden durch einen Content-Scanner bereits am Eingang auf bedenkliche Inhalte geprüft. Wenn zweifelsfrei festgestellt wird, dass dieser zur Kategorie „unerwünscht“ gehört, werden solche e-Mails nicht zugestellt.
- Der Einsatz eines URL-Filters stellt sicher, dass URLs, hinter denen sich die Kollektoren von Phishing-Attacken verstecken, von Benutzern gar nicht besucht werden können – sollte trotz e-Mail Scanning dennoch ein Phishing-Mail am Arbeitsplatz landen.

Der URL-Filter und seine mehrmals täglich durch den Hersteller aktualisierte Datenbank (aller als gefährlich eingestuften Links) verhindern den Verbindungsaufbau zu den entsprechenden Webservern.

Mehr über aktuelle Trends im IT-Security Bereich und wie Sie sich vor neuen Bedrohungen schützen können, erfahren Sie auf dem nächsten Bacher Systems Breakfast am 7. September 2006 (siehe umseitiger Kasten).

Trainings bei Bacher Systems

IT-Infrastruktur

Unix Grundlagen der Solaris 10 Betriebssystemumgebung
4.9. - 7.9.2006 / € 1.990,-

Solaris 10 OE Systemadministration I
11.9. - 15.9.2006 / € 2.790,-

Solaris 10 OE Systemadministration II
18.9. - 22.9.2006 / € 2.790,-

Sun Cluster Verwaltung
18.9. - 22.9.2006 / € 3.890,-

Solaris 10 für erfahrene Systemadministratoren
25.9. - 29.9.2006 / € 2.790,-

IT-Sicherheit

Accelerated CCSE NGX - Upgrade Training
11.9. - 12.9.2006 / € 1.350,-

Intensiv Workshop: SecurePlatform
13.9.2006 / € 690,-

Check Point Security Administration NGX I
25.9. - 26.9.2006 / € 1.350,-

Check Point Security Administration NGX II
2.10. - 4.10.2006 / € 1.990,-

Alle Preise pro Person exkl. MwSt.

Firmenspezifische Kurse auf Anfrage.
Anmeldungen: training@bacher.at

Kursinfos: www.bacher.at/training

**Package
NGX I+II
€ 2.900,-
statt € 3.340,-**

Änderungen vorbehalten

Bacher Systems EDV GmbH, 1100 Wien, Clemens-Holzmeister-Straße 4, Tel.: +43.1/60 126-0, Fax: +43.1/60 126-4, E-Mail: info@bacher.at

