SecureNet

DIE SEMANTISCHE EBENE DER SICHERHEIT VON WEBANWENDUNGEN

Über die unbegrenzten Möglichkeiten für Täuschung und Betrug im Web

Whitepaper – SecureNet GmbH, Mai 03

1 EINLEITUNG

Nach wie vor ist die Sicherheit vieler Internetsites auf einem Niveau, welches modernen Betrügern das Handwerk äußerst leicht macht. So existiert auf vielen Sites ein ganz bestimmtes Sicherheitsloch, das ausgenutzt werden kann, um bei Banken die PINS und TANS zu stehlen, bei Zeitungen und Zeitschriften gefälschte Artikel zu plazieren, bei e-Business Anwendungen in den Besitz der Zugangsdaten zu kommen, auf den Sites seriöser Unternehmen Viren und Trojaner zum Download bereitzustellen oder um Ruf und Geschäft zu schädigen – um nur einige Beispiele zu nennen.

Fast allen namhaften Websites läßt sich heutzutage bescheinigen, dass bei Gestaltung und Bedienerführung weder Kosten noch Mühen gescheut worden sind. Für den Experten ist aber ebenso klar ersichtlich, dass für den Schutz vor Betrug und Täuschung in erschreckend vielen Fällen kaum etwas getan worden ist.

Mit diesem Papier möchten wir an einigen Beispielen schildern, welche Gefahren drohen. Die den Beispielen zugrundeliegenden Voraussetzungen sind real und auf einer großen Zahl von Websites namhafter Unternehmen anzutreffen.

Eine solche Darstellung bringt es naturgemäß mit sich, dass sie in einer entsprechenden Interessenslage befindliche Menschen überhaupt erst auf die Idee bringt, diesen oder jenen 'Trick' einmal anzuwenden. Selbstverständlich wollen wir hier niemanden anstiften. Nur verhält es sich auch hier so, wie bei allen IT-Sicherheitsfragen: Die gegnerische Seite wird irgendwann darauf kommen. Und dann ist es besser, man ist bereits gewarnt und die Technik hält nicht unbemerkt Einzug in die Trickkiste des Angreifers.

2 Die zugrundeliegende Sicherheitslücke: Cross-Site Scripting

Den in diesem Papier behandelten Angriffen liegt das sogenannte Cross-Site-Scripting, kurz XSS, zugrunde. Immer dann, wenn Benutzereingaben in die nach dem Absenden angezeigte Antwortseite ungefiltert eingebaut werden, ist das XSS-Loch da. Warum? Weil der Benutzer z.B. HTML-Code in das Eingabefeld eingeben könnte. Bestes Beispiel: Die Suchfunktion. „Zu dem Suchbegriff ‚`nähmlich`' wurde leider kein Treffer gefunden“ heisst es da z.B. als Antwort. Geben wir statt `nähmlich` doch einmal `<I>Gieraffe`,

mit dem i in spitzen Klammern als HTML-Code für Kursivschrift, in das Suchfeld ein. Und schon erscheint in der Antwortseite der Text *Gieraffe* und alles, was danach kommt, kursiv. Peinlich für den Programmierer, aber noch nicht weiter tragisch. Das wird es aber dann, wenn wir auf diese Weise Texte übergeben, die den Inhalt der Seite verfälschen. Mittels bestimmter HTML-Konstrukte ist es überdies möglich, die gesamte Seite oder Teilflächen zu überdecken, sie mit Eingabefeldern und Absende-Buttons auszustatten, so dass die gemachten Eingaben auf der Seite des Angreifers landen. Und all das wird transportiert per Email, versteckt hinter einem unverdächtig aussehenden Link.

Eine andere Gefahr ergibt sich aus der Möglichkeit, auf die beschriebene Weise JavaScript-Befehle zu übergeben. Die Übergabe von `<script>alert(document.cookie)</script>` beispielsweise führt dazu, dass im Browser des Users das kleine graue Fenster hoch poppt und das Cookie anzeigt, das diese Site zuvor gesetzt hat. Auf diese Weise sind eine ganze Reihe von Angriffen und Täuschungen des Users möglich. Statt das Cookie nur anzuzeigen, kann es genauso einfach an den Hacker transferiert, also gestohlen werden. Der kann sich damit in bestehende Webmail-, Onlinebanking- oder sonstige Sitzungen einschleichen.

Damit eine Webseite in der beschriebene Weise verändert werden kann, muss dem Internetnutzer ein entsprechender Link untergeschoben werden. Dies geschieht entweder durch den Versand einer HTML-formatierten Email an das Opfer oder dadurch, dass der Benutzer auf eine vom Angreifer kontrollierte Website gelockt und dort zum Klick auf den 'verschmutzten' Link verleitet wird. In dem einfachen obigen Beispiel würde der Link, um den nachfolgenden Text auf der Suchseite kursiv erscheinen zu lassen, etwa so aussehen:

```
http://www.website.tld/suche?text=<i>Gieraffe
```

Ein Angreifer würde diesen Link hinter einer passenden Bezeichnung verstecken. Die folgenden Beispiele zeigen die Anwendung diese Prinzips in weniger trivialen Fällen.

3 DAS SZENARIO

Vorab illustrieren wir auf nicht-technischem Niveau das Verfahren, auf dem die im folgenden beschriebenen Angriffe beruhen.

Ich bin – sagen wir – Kunde einer Bank. Meine Bank schickt mir einen Brief, ganz normal per Post, in dem sie mich z.B. über Änderungen in der Kontoführung aufklärt. Sie bittet mich da etwa um Ausfüllen und Rücksendung des dem Schreiben beiliegenden Formulars oder darum, die genannten Hinweise zu berücksichtigen. Ein ganz normaler Prozess, wir alle wissen, wie wir damit umgehen müssen. An der Authentizität zu zweifeln kommt wohl niemandem mehr in den Sinn. Wir tun, was von uns verlangt wird.

Ganz anders in der schönen neuen Online-Welt. Wir bekommen eine Email. Statt des Formulars einen Link auf eine Internetseite mit der Anweisung, dies oder das dort zu erledigen. Hier kommt nun doch ein wenig Misstrauen hoch. Wir prüfen genauer: Als Absender der Name der Bank, der angegebene Link zeigt deutlich auf die Website der Bank und der Text klingt sehr plausibel und authentisch. Überzeugt! Wir klicken auf den Link und landen tatsächlich auf der Website unserer Bank, in der uns vom Online-Banking vertrauten Umgebung. Spätestens jetzt wird die Mehrzahl der so angeschriebenen alle Skepsis abgelegt haben und sich den Anweisungen fügen. All zu schnell zeigen wir in der Online-Welt dasselbe Verhalten, das

uns in der ‚richtigen' Welt antrainiert und worden ist und das wir als sinnvoll erkannt haben. Wir gehen unbewusst von denselben Annahmen aus und hinterfragen diese nicht mehr.

Und genau hier liegt das Problem. Eine Email zu fälschen ist problemlos möglich, sie an eine große Anzahl von Opfern zu versenden ohne nennenswerte Kosten und mit wenig Aufwand durchführbar. Und mit der auf vielen Websites vorkommenden XSS-Lücke ist es möglich, in einer Email versteckt beliebige Inhalte zu übermitteln, die dann tatsächlich auf der Original-Website angezeigt werden und dadurch eine entsprechende Authentizität erlangen.

Bei XSS handelt es sich um ein Problem, das seit mehreren Jahren bekannt ist, dessen Gefahren man aber bisher als gering eingeschätzt hat bzw. ausschließlich in dem Zusammenhang des Session-Hijackings gesehen hat. Es ist erschreckend, auf wie vielen Websites es nach wie vor anzutreffen ist und damit Angriffe der hier beschriebenen Art ermöglicht.

Zusammengefasst: Alle im folgenden geschilderten Betrügereien nutzen einerseits die Unsicherheiten von Emails und das falsche Vertrauen der User in deren Authentizität, andererseits das XSS-Sicherheitsloch in vielen Webauftritten und –anwendungen, das es erlaubt, fast beliebige Inhalte auf der Website zu plazieren.

4 BEISPIEL 1: ONLINE BANKING

Unser Ziel

Wir wollen in den Besitz der Zugangsdaten (zumeist UserID, PIN) und einer frischen TAN kommen, um uns damit unter der Identität des Users beim Onlinebanking anzumelden und eine Überweisung zu veranlassen.

So gehen wir vor

Wir schicken einer möglichst großen Zahl von Onlinebanking-Kunden einer Bank, von der wir wissen, dass sie ein geeignetes Sicherheitsloch besitzt – z.B. das oben erwähnte – eine Email folgender Form:

```
Sehr geehrter Meinebank-Kunde,

wir haben unser Online-Banking noch sicherer
gemacht. Damit Sie möglichst schnell in den Genuß
der neuen Sicherheit gelangen, bitte wir Sie, diese
für Ihr Konto noch heute freizuschalten. Bitte
klicken Sie hier und folgen Sie den Anweisungen.

http://banking.meinebank.de/securitycheck

...

Vielen Dank

Ihr Meinebank-Kundenservice
Service/Mailformular: http://www.meinebank.de/help
```

Der angegebene Link führt den User zwar auf die Site seiner Bank, allerdings auf eine Seite, die von uns unter Ausnutzung des besagten

Sicherheitsloches manipuliert worden ist. Auf dieser Seite findet der Benutzer nun die Anmeldemaske, in die er seine Zugangsdaten (UserID und PIN o.ä.) eintragen muß – ganz so, wie er sie von unzähligen Online-Sitzungen her kennt. Allerdings mit dem Unterschied, dass die Daten nicht zur Bank gelangen, sondern dorthin, wo wir sie später abgreifen können, z.B. einem öffentlichen und anonym zugreifbaren Server. Damit wir Transaktionen auslösen können, benötigen wir noch mindestens eine TAN. Wir fordern daher den Benutzer auf, zur Bestätigung eine TAN einzugeben (wir weisen ihn darauf hin, nicht zu vergessen, diese TAN aus seiner Liste zu streichen). Auch das wird die meisten User nicht weiter wundern, sind sie daran doch bei bestimmten Aufträgen gewöhnt.

Jetzt holen wir uns die auf dem öffentlichen Server abgelegten Zugangsdaten ab und nehmen die frisch gewonnene Online-Identität ein: Wir loggen uns (damit eine Rückverfolgung nicht möglich ist über einen anonymisierenden Proxy) bei der Bank ein und tätigen eine beliebige Überweisung. Die dazu erforderliche unverbrauchte TAN haben wir ja.

5 BEISPIEL 2: GEFÄLSCHTE ZEITUNGSMELDUNG

Unser Ziel

Wir möchten ein Täuschungsmanöver dadurch erleichtern, dass wir unsere Aussagen von einem als seriös und vertrauensvoll eingestuften Dritten bestätigen lassen, beispielsweise einer angesehenen Zeitung. Wir verschaffen uns sozusagen den geeigneten *Vertrauenskontext*.

So gehen wir vor

Wir verschicken wieder eine Mail, z.B. in dieser Form:

```
Sehr geehrte Frau ...,

wie freuen uns Ihnen mitteilen zu können, dass Sie
in unserem Preisausschreiben gewonnen haben. Ihr
Preis:

Rang: 512
Preis: 200 €

Bitte geben Sie uns Ihre Kontoverbindung (BLZ,
Konto, Kontoinhaber) an, damit wir Ihnen den Betrag
überweisen können. Dies können Sie durch Antwort
auf diese Email tun oder mit sicherer Übertragung
unter http://www.PROMINENTEFIRMA.de/dateneingabe.

Nähere Informationen zur Ausschüttung entnehmen Sie
bitte dem Artikel in der Bekanntezeitung vom 12.4.,
den Sie auch online finden unter:
http://www.bekanntezeitung.de/wirtschaft/B2/702

Ihr Anrecht auf den Preis verfällt laut unseren
Bedingungen, wenn wir nicht bis zum 1.7.03 alle für
die Zustellung des Preises erforderlichen
Informationen von Ihnen erhalten haben.

Mit freundlichen Grüßen
Ihr ...-Team und unser Sponsor PROMINENTEFIRMA
```

Hier werden gleich zweimal angesehene Namen benutzt, um Glaubwürdigkeit zu erreichen: Der Link auf den Online-Artikel einer

bekannten Publikation verleiht der Story eine kaum schlagbare Authentizität. Und die Benutzung der Website einer bekannten Firma (die das besagte Sicherheitsloch enthält) überträgt das Vertrauen, das mit der Seriosität dieser Firma verbunden ist, auf die eigenen, in hohem Masse unseriösen Absichten.

Wozu könnte diese Aktion nützlich sein? Z.B. dazu, um an die Kontoverbindungen zu kommen, die wir in obigem Online-Banking-Beispiel benötigen.

Nach demselben Schema sind unzählige Betrügereien denkbar. Fast alle Tricks aus der richtigen Welt lassen sich ins Internet übertragen und hier auf diese Weise von anerkannter Seite beglaubigen. Das kommt etwa dem gleich, dass der Betrüger – etwa der vermeintliche Vermögensberater mit dem todsicheren Anlagetip – mit der (gefälschten) Börsenzeitung unter dem Arm vorbei kommt, in der seine Aussagen untermauert werden.

6 BEISPIEL 3: VIREN

Ein neuer Weg, Viren, 190er-Dialer oder andere schädliche Software zu verbreiten, ist dieser:

> Sehr geehrter Internet-Nutzer,
>
> wie Sie vielleicht schon der Presse entnommen haben, hat das MINISTERIUM_ODER_AMT_ODER_POLIZEI eine umfassende Initiative gegen Computerkriminalität, insbesondere im Zusammenhang mit den sog. 190er-Dialern, gestartet.
>
> ...
>
> Wir möchten Sie daher auffordern, sich einmal auf unserer Website umzusehen und möglichst auch den dort angebotenen Dialer-Filter
>
> www. MINISTERIUM ODER AMT ODER POLIZEI.de/ sicherheit/dialerschutz.exe
>
> herunterzuladen. Die Installation ist sehr einfach und hat keinerlei Auswirkungen auf Ihr System. Evtl. ist es erforderlich, dass Sie Ihre Anti-Virus Software vorher ausschalten, da manche ältere Versionen einen Virus melden.
>
> Die Zeitschrift BEKANNTE-COMPUTERZEITSCHRIFT hat unserer Software jüngst getestet und ihr das Prädikat ‚Absolut empfehlenswert' verliehen. Den Test und weitere nützliche Tips können Sie auch direkt im Internet nachlesen unter: www.BEKANNTE COMPUTERZEITSCHRIFT.de/test/2231/index .html.
>
> Wir würden uns freuen, wenn unsere neue Website zukünftig zu den Zielen gehört, die Sie regelmäßig besuchen.
>
> Ihr Sicherheitsteam von ____

Angenommen, der Empfänger dieser eMail wird mißtrauisch („Woher haben die meine Adresse?“, „Verschicken die jetzt auch schon SPAM?“), welche Prüfungen wird er vornehmen, um sich der Authentizität zu versichern?

- Der Absender der Mail lautet initiative2004@ MINISTERIUM_ODER_AMT_ODER_POLIZEI.de. das klingt hinreichend vertrauenswürdig
- Der Link zeigt auf die Original-Website. Klick auf den Link oder Eingabe der Homepage führt tatsächlich auf die Site und spätestens nach dem Herumklicken auf der Site wird die Gewissheit eintreten, dass sie echt ist. Auch das Zertifikat, das bei sicherer https-Verbindung über die Authentizität der Site Auskunft gibt, würde echt sein.

Der Link zum Test einer Computerzeitschrift wird schliesslich jeden noch verbleibenden Rest von Zweifel wegwischen. Und das eindeutige Urteil der Zeitschrift wird zusätzlichen Anreiz geben, diese Software auch tatsächlich gleich zu installieren, kommt sie doch mit einer seriösen Absenderangabe und ist auch noch von einer anerkannten Fachzeitschrift für gut befunden worden.

Dem Hinweis, die Virensoftware vorher auszuschalten, wird man nun wahrscheinlich ohne weiter ins Grübeln zu geraten, Folge leisten bzw. beim Anspringen des Virenschutzes nicht weiter erschrocken sein.

Wir können uns mittlerweile denken, dass die Email falsch und die Adresse gefälscht ist und dass sowohl der Link auf die Download-Site als auch der Link zur Zeitschrift den Code zur Ausnutzung der beschriebenen Sicherheitslöcher in sich tragen. Und dass die vermeintliche Schutzsoftware genau das Gegenteil ist. Die für Hacker immer größer werdende Hürde, Virensoftware ins Ziel zu bringen, wird auf elegante Weise umgangen. Die Mail läßt sich in kürzester Zeit an Hunderttausende oder Millionen Empfänger verschicken. Ein Satz wie „Sie helfen unserer Sache, wenn Sie diese Mail an Bekannte und Freunde weiterleiten.“ würde die Anzahl beträchtlich erhöhen.

Um den geeigneten Vertrauenskontext herzustellen, kommt eine Vielzahl von Institutionen in Frage. Eine einzige unter ihnen mit der besagten XSS-Lücke reicht aus, um den hier beschriebenen Schaden in voller Breite anzurichten.

7 BEISPIEL 4: E-BUSINESS

Die Anzahl der Unternehmen, die Geschäftsprozesse mit dem Prädikat „mission-critical“ über das Internet abwickeln, wird immer größer. Zwar läuft der Zugriff fast immer über eine verschlüsselte Verbindung ab (das Zertifikat schützt hier nicht, es wird bei dieser Angriffsform nicht verletzt), erschreckend aber ist, wieviele dieser Sites als Zugangsschutz die auf UserID und Password beruhende Authentifizierung einsetzen. Das bloße Ausspähen genügt, um in die elektronische Identität des betreffenden Users zu schlüpfen. Wie leicht das ist, machen obige Beispiele sicher bereits deutlich.

Waren es bei den anderen Beispielen einzelne Personen, die sich bereichern oder einfach nur Schaden anrichten wollen, so geht es hier um das Thema Wirtschaftsspionage und Sabotage.

Ein Beispiel

Ein Unternehmen (Bsp: ein Pharmagroßhändler) möchte Informationen über die Lieferantenbeziehung – Rabatte, Umschlagsmengen usw – zwischen

einem Konkurrenten (also ein anderer Pharmagroßhändler) und dem gemeinsamen Lieferanten (dem großen Pharmaunternehmen) erlangen. Am einfachsten erreicht es das durch Nutzung des E-Business Portals des Lieferanten.

Wie nehmen an, dass der Industriespion von der B2B-Anwendung nicht viel mehr weiss als die bloße Tatsache, dass der Lieferant sie betreibt sowie das, was aus der Homepage oder den öffentlichen Seiten ersichtlich ist. Um das Konto der Konkurrenz einsehen zu können, ist zunächst die Person – genauer: die Emailadresse dieser Person – herauszufinden. Das läßt sich sicher auf vielfältige Weise, also z.B. ganz klassisch mittels Durchfragen per Telefon, bewerkstelligen. Im Besitz der Emailadresse, schickt unser Spion aber viel einfacher und risikoloser eine Email mit gefälschter Absenderadresse und in etwa folgendem Wortlaut ab:

```
Sehr geehrte Handelspartner und Portalnutzer,

wie Ihnen sicher bekannt ist, führen wir an jedem
Sonntag routinemäßige Wartungsarbeiten an unseren
Servern durch. Bei den gestrigen Arbeiten haben
sich leider Fehler eingeschlichen, die bei einigen
Benutzern unter ungünstigen Umständen dazu führen
können, dass deren Zugang blockiert ist. Aufgrund
Ihres Benutzerprofils gehören Sie leider zu dem
Kreis der gefährdeten Nutzer. Um Ihnen eine
störungsfreie weitere Benutzung unseres Portals zu
ermöglichen, möchten wir Sie daher bitten, kurz zu
prüfen, ob Ihnen der Zugang nach wie vor möglich
ist und ihn ggf. erneut freizuschalten. Dazu
brauchen Sie nur auf diesen Link

http://portal.CHEMIEKONZERN.de/support/checkaccount

zu klicken und sich an Ihrem Konto anzumelden.
Gelingt die Anmeldung, sind Sie nicht betroffen und
brauchen nichts weiter zu tun. Im anderen Fall
geben sie einfach ein neues Passwort ein und die
Sache ist ebenfalls wieder behoben.

Wir bedauern diese Unannehmlichkeit und danken
Ihnen für Ihre Unterstützung.

Mit freundlichen Grüßen

Ihr ___ Service Team.
```

Die Zugangsdaten lassen sich nun nutzen für Aktivitäten wie:

- Beobachtung und Auswertung der Bestellvorgänge über einen beliebigen Zeitraum.
- Blockieren des Zugangs für den legitimierten User durch Passwortänderung
- Veränderung von Bestellmengen oder Aufgeben von neuen Bestellungen

8 BEISPIEL 5: WEBMAIL

Um an die Zugangsdaten eines Users zu seinem Webmail-Account zu gelangen, schicken wir ihm eine Mail – an diesen Webmail-Account – in der wir ihn dazu verleiten, auf einen Link zu klicken. Dieser Link führt ihn auf eine gefälschte Website, die genauso aussieht wie sein Webmailanbieter, in der berechtigten Hoffnung, dass er nicht merkt, dass sie gefälscht ist. Dort

wird ihm gesagt, dass seine Sitzung wegen eines Systemfehlers oder aus Sicherheitsgründen abgelaufen ist (so etwas ist ja durchaus Gang und Gäbe und wohl jeder wird dies schon einmal erlebt haben) und dass er sich erneut anmelden soll. Nachdem der User dies getan hat, leiten wir ihn – nun im Besitz seiner Zugangsdaten – auf die richtige Site zurück. Das Schlimmste, was uns passieren kann, sollte der User Verdacht geschöpft haben, ist, dass er darauf gleich sein Passwort ändert und wir mit seinen Zugangsdaten nichts mehr anfangen können.

Mit den Zugangsdaten können wir nun nicht nur – schlimm genug – nach Belieben in den Emails des User herumschnüffeln. Wir können mehr. Zum Beispiel:

Passworte anderer Dienste ermitteln

Es hat sich mittlerweile eingebürgert, dass Webdienste unter dem Stichwort ‚Passwort vergessen?' dem User auf Anforderung sein Passwort an die hinterlegte Emailadresse senden. Man geht von der Annahme aus, dass nur der User selbst Zugriff auf sein Emailpostfach hat, und mithin das Passwort durch Zusenden in den richtigen Händen landet. Lassen wir einmal beiseite, dass diese Annahme eine Reihe anderer Sicherheitsmängel aufweist. Auf jeden Fall verschafft uns, im Besitz des Zugangs zum Webmail-Account des Opfers, dieses Verfahren eine Möglichkeit, auf sehr einfache Weise an weitere Passworte zu gelangen. Wir fordern die Zusendung einfach bei dem Dienst an, von dem wir meinen, dass unsere Opfer dort registriert ist. Entsprechende Hinweise darauf finden sich sicher auch irgendwo in den Emails. Nach Erhalt löschen wir die Mail sofort, so bleiben keine Spuren zurück.

Registrierung bei Internet-Diensten mit der Identität eines Anderen

Es kann viele Gründe dafür geben, dass wir uns bei einem Internet-Dienst statt unter einem anonymen Namen unter dem Namen einer bestimmten Person anmelden möchten. Um Missbrauch zu erschweren, versenden diese Dienste, nachdem der User die Registrierungsdaten eingegeben hat, eine Bestätigungsemail an die angegebene Emailadresse. Erst wenn der User auf den in der Email genannten Link klickt bzw den darin übermittelten Code eingibt, ist die Registrierung erfolgreich abgeschlossen. So wird sichergestellt, dass die Emailadresse auch tatsächlich demjenigen gehört, der sich da angemeldet hat. Wir wissen mittlerweile, dass diese Annahme falsch ist. Sind wir im Besitz des WebMail-Kontos, können wir auch hier, ohne Spuren zu hinterlassen, frei agieren.

Es stellt sich die Frage, als wie beweiskräftig ein Richter dieses Nachweisverfahren einstuft, wenn dem vermeintlichen User später etwas angelastet wird.

Konto sperren

Durch einfaches Ändern des Passwortes oder Löschen des gesamten Accounts kann bei Personen, die ihren Webmail-Acount geschäftlich nutzen, beträchtlicher Schaden angerichtet werden.

9 ZUSAMMENFASSUNG

Die obigen Beispiele – sie sind nur ein kleiner Auszug aus der Bandbreite der vorhandenen Möglichkeiten – haben gezeigt, wie leicht es ist, die Identität einer anderen Person einzunehmen und damit Schaden anzurichten. Der Täter hat es leicht,

— im Namen eines anderen Unrecht oder Straftaten zu begehen

- jemanden gezielt zu schädigen, etwa um „alte Rechnungen“ zu begleichen
- an Informationen zu gelangen, an die er unter seiner richtigen Identität niemals kommen würde.
- Dritte zu Handlungen zu bewegen oder zu verleiten, zu denen er sie sonst nicht verleiten könnte.
- andere Personen auszuspionieren
- öffentlich zugängliche Informationen zu manipulieren

Möglich wird dies einerseits durch die breite Verwendung einer unsicheren Authentifizierungsmethode, die zum Nachweis der elektronischen Identität lediglich die Kenntnis einer User-ID und eines Passwortes voraussetzt. Zum anderen dadurch, dass viele Websites ein Sicherheitsloch aufweisen, welches die oben genannten Techniken und Tricks erst ermöglicht.

Die Anwender sind angesichts der Schwächen der heutigen Webtechnologien nicht in der Lage, sich ausreichend zu schützen. Deshalb müssen die Anbieter – auch im eigenen Interesse – Verantwortung für die Sicherheit ihrer Kunden übernehmen und dafür Sorge tragen, dass ihre Anwendungen sicher sind, Die Web Application Security ist als selbstverständlicher Bestandteil in die Qualitätssicherungsprozesse zu integrieren.

Weitere Informationen

SecureNet GmbH

Münchner Technologiezentrum
Frankfurter Ring 193a
80807 München

Web: http://www.securenet.de
Email: info@securenet.de
Tel: (+49) 89 - 32133-600

Sicherheit auf Anwendungsebene ist völlig anderer Natur als die klassische Netzwerksecurity – und sie ist um Einiges komplexer. Um WAS für eine Webanwendung sicherstellen zu können, ist ein ebenso breites wie tiefes Verständnis der Praxis der Softwareentwicklung erforderlich. Die SecureNet GmbH ist ein Internet-Softwarehaus mit vielen Jahren Erfahrung in der Entwicklung von eBusiness-Anwendungen – mit dem Focus auf Security. Lange bevor *Web Application Security* eben diesen Namen erhalten hat, haben wir sie uns zu eigen gemacht. Wir sagen Ihnen nicht nur, was Sie tun müssen, um die beschriebenen Sicherheitslöcher zu schliessen, sondern helfen Ihnen auch, die Sicherheit Ihrer Webanwendungen umfassend und dauerhaft herzustellen.