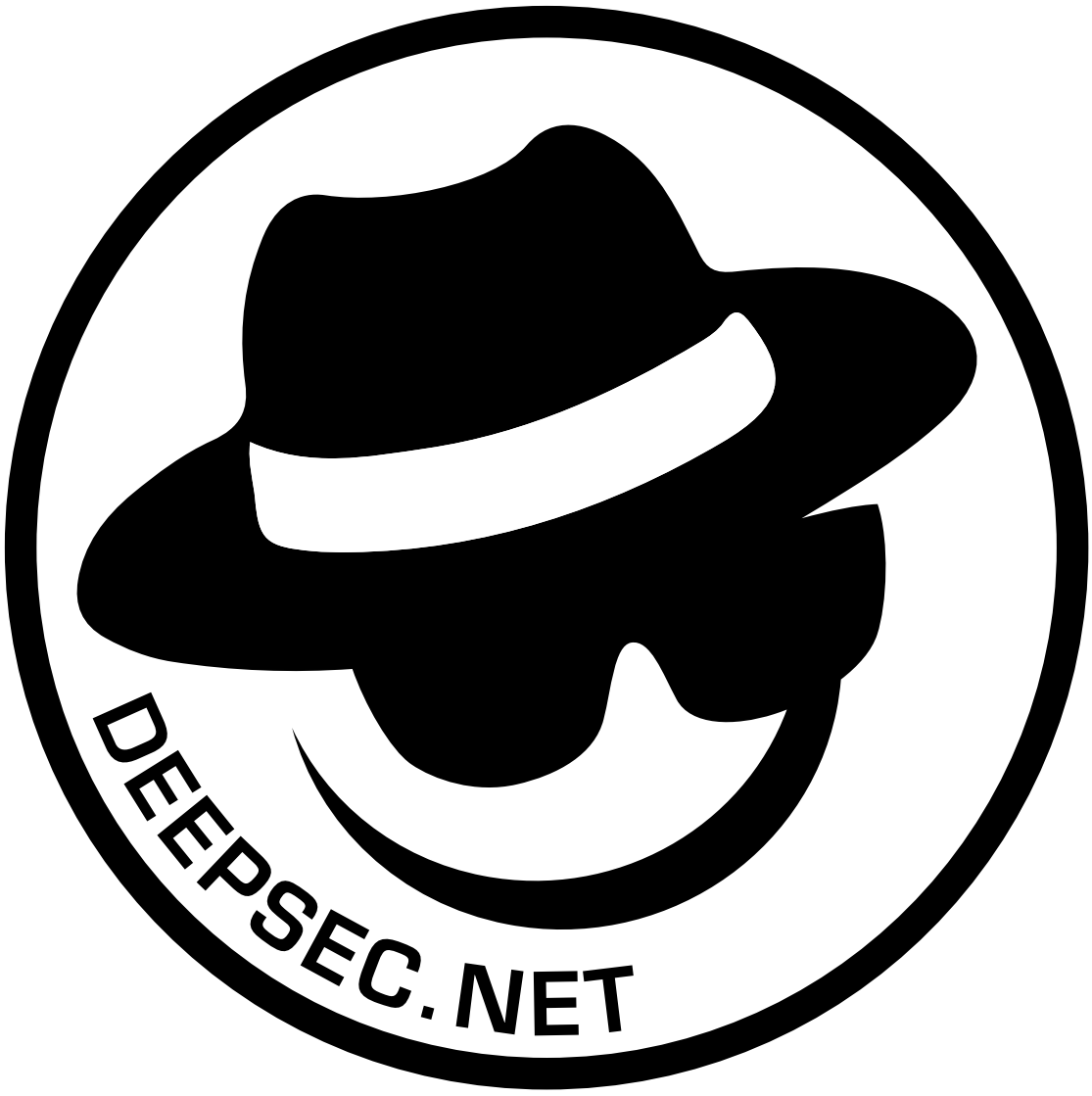


press review 2012

contents

media coverage

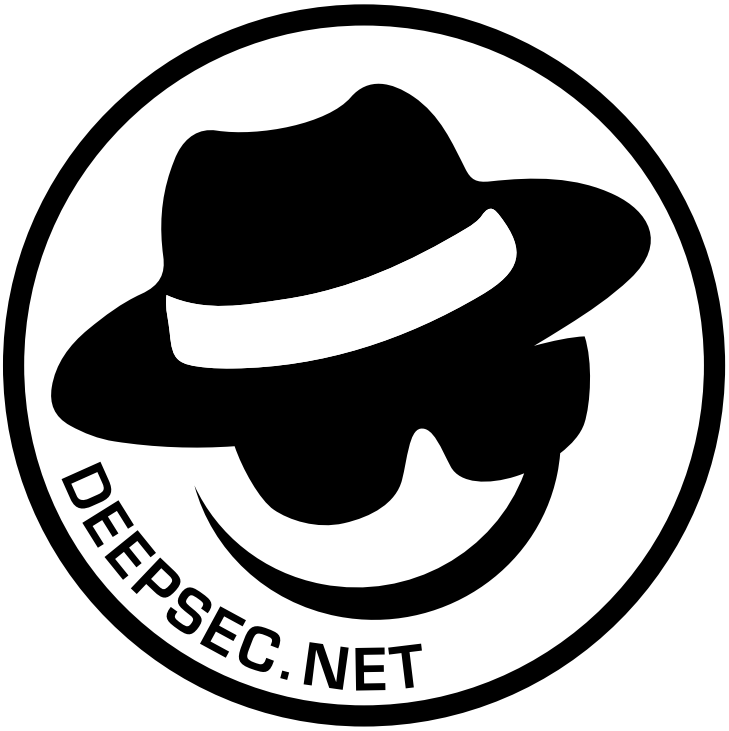
2012

press releases

2012

contact / impressum

media coverage 2012



http://www.golem.de/news/2012-die-verschwindetricks-der-social-engineers-1212-96455.html

Die Verschwindetricks der Social Engineers

Datum:26.12.2012

Autor:Jörg Thoma

Per Social Engineering ist es Betrügern 2012 gelungen, die gesamte digitale Identität eines Wired-Journalisten verschwinden zu lassen. Im Real Life ließen sie sogar eine ganze Brücke mitgehen.

Jenseits von Phishing-Attacken, als Nacktfotos getarnter Malware im E-Mail-Postfach oder sprachlich unbeholfenen Aufforderungen, bei lukrativen Finanztransaktionen in Nigeria behilflich zu sein, gibt es Betrugsmaschen, auf die selbst Polizei und IT-Experten hereinfallen: Hacks auf Onlinekonten, Identitätsklau, Industriespionage, Diebstahl mit digitalen Unterschriften oder mit gefälschten Dokumenten. Die Social-Engineering-Expertin und Sicherheitsprüferin Sharon Conheady hat auf der Deepsec 2012 die spektakulärsten Scams 2012 präsentiert.

http://video.golem.de/internet/6440/interview-sharon-conheady.html
Video: Interview Sharon Conheady über Social Engineering (10:41)

Gesamtes digitales Leben gelöscht

Das komplette digitale Leben des Wired-Journalisten Matt Honan wurde von Angreifern gelöscht. Sie verschafften sich durch Social Engineering genügend Informationen, um sich bei einem Anruf beim Apple-Support als Honan zu authentifizieren und forderten ein neues Passwort für Honans Me.com-Account an. Damit ausgestattet, konnten sie gleich auch Honans Apple-ID ändern. Zuvor hatten sie noch die Bestätigungs-E-Mail in den Papierkorb verschoben. Kurz darauf setzten sie sein Gmail-Passwort und die Zugangsdaten zu seinem Konto bei Google zurück. Kleinlaut musste Honan zugeben, dass es ein Fehler gewesen war, sämtliche E-Mail-Konten mit dem gleichen Namen zu versehen und sie auch mit verschiedenen Konten zu verknüpfen. Backups hatte er nicht. Hätte er seinen Google-Account mit zweifacher Authentifizierung abgesichert, wären die Hacker nicht weitergekommen, schreibt er in einem ausführlichen Bericht. Er kritisierte aber auch Apple, das mit nur wenigen Informationen das Zurücksetzen eines Passworts erlaubt.

Ziel der Scammer war das Twitter-Konto

Auch das Passwort für Honans Twitter-Account forderten die Hacker an und verbreiteten darüber rassistische Tweets. Über den iCloud-Account setzten sie iPhone, iPad und Macbook zurück und löschten schließlich auch sein Google-Konto. E-Mails, Familienfotos, alles sei weg, beklagt Honan. Die Angreifer hatten es zwar nur auf sein Twitter-Konto abgesehen, löschten aber alles andere, damit Honan ihn nicht wieder zurückbekommen würde.

Letztendlich benötigt Apple nur die Rechnungsadresse und die letzten vier Zahlen der Kreditkarte, um einen Zugang zurückzusetzen, wie das Unternehmen auf Anfrage von Wired bestätigte. Wie die Betrüger daran gekommen waren, erfuhr Honan später von ihnen selbst. Sie tauschten sich über Honans neuen Twitter-Account aus.

Erst Amazon-, dann Google- und Apple-Konten

Honans Rechnungsadresse erfuhren die Hacker durch einen einfachen Whois-Lookup seiner privaten Domäne. Genauso gut hätten sie aber öffentliche Verzeichnisse im Internet durchforsten können, schreibt Honan. Den wiederkehrenden Namen "mhonan" in seinen diversen E-Mail-Adressen erfuhren sie über seinen Twitter-Account.
Die benötigten Ziffern seiner Kreditkartennummer holten sich die Hacker bei Amazon. Dort hatte Honan ebenfalls ein Konto. Zunächst riefen die Betrüger beim Support an und gaben die Rechnungsadresse, die E-Mail-Adresse und den Namen an. Nach erfolgreicher Authentifizierung verlangten sie, dem Konto eine zweite Kreditkartennummer hinzuzufügen, und gaben eine - natürlich gefälschte - Nummer durch.
Später riefen sie nochmals dort an, gaben an, keinen Zugang zum Konto mehr zu haben und gaben wieder Rechnungsadresse, Name, E-Mail-Adresse und die neue Kreditkartennummer an. Daraufhin konnten sie dem Konto eine zweite E-Mail-Adresse hinzufügen, an die dann ein neues Passwort versendet wurde. Damit ausgestattet, loggten sie sich ein und erfuhren die Ziffern, die sie für die Authentifizierung bei Apple benötigten.

Es war nicht persönlich gemeint

Sie hätten es nicht auf ihn persönlich abgesehen, schrieb ihm einer der Betrüger später. Sie hätten nur sein Twitter-Konto kapern wollen. Es hätte schlimmer kommen können, schrieb der zerknirschte Journalist, denn er habe zahlreiche einflussreiche Namen in seiner Kontaktliste, die ebenfalls hätten angegriffen werden können. Er trauere aber um die unwiederbringlich gelöschten Fotos seiner Familie, vor allem seiner kleinen Tochter, die er seit ihrer Geburt gesammelt hatte. Auch sein Ruf als IT-Journalist habe gelitten.
Dem Hacker habe sein Tun später leidgetan, schreibt Honan. Nicht er, sondern sein Kumpel habe Honans Daten gelöscht, teilte der Angreifer mit. Auf die Frage Honans, warum er den Hack eigentlich durchgeführt habe, antwortete er lapidar, er wolle auf die Schwachstelle hinweisen. Die Hackerethik besagt allerdings, dass öffentliche Daten genutzt und private Daten geschützt werden müssen.

Falscher Paul Allen verschafft sich Kontozugang

Stars oder Millionäre sind natürlich ein beliebtes Angriffsziel für Scammer, da über sie viel bekannt ist und das Hacken eine medienwirksame Aktion bedeutet - oder einfach, weil sie viel Geld haben.
Nicht besonders geschickt hat sich ein unerlaubt abwesender US-Soldat in den USA angestellt, der sich zunächst

erfolgreich als der Millionär und Microsoft-Mitbegründer Paul Allen ausgab. Er rief bei Allens Bank an und erklärte, dass er seine Bankkarte daheim verlegt hätte. Er wolle die Karte zwar nicht als verloren melden, hätte aber gerne sobald wie möglich eine zweite. Der Citibank-Mitarbeiter war offensichtlich so hilfsbereit, dass er eine zusätzliche Adresse aufnahm, an die er die zweite Karte per Express rausschickte. Der US-Soldat gab auch gleich seine Telefonnummer an.

Viel Erfolg hatte der Soldat aber nicht. Ihm gelang zwar zunächst eine Überweisung in Höhe von etwa 600 US-Dollar mit der neuen Karte, eine zweite Überweisung in Höhe von 15.000 US-Dollar sowie Einkäufe in einem Computerspielgeschäft fielen aber der Betrugsabteilung in der Bank auf. Der Soldat wurde verhaftet und angeklagt. Wie der Betrüger den Bankmitarbeiter dazu überredete, die zweite Karte auszustellen, bleibt ein Geheimnis. Die Bank gab dazu keinen Kommentar ab.

Mit öffentlicher Unterschrift zu Millionen

Gleich mehrere Anläufe benötigten Scammer aus Hongkong, um etwa 2 Millionen US-Dollar zu erbeuten. Das Geld ergaunerten sie von Wells Fargo, das ein gemeinsames Treuhandkonto des US-Bezirks Merced und der Catholic Healthcare West verwaltet. Das Geld auf dem Treuhandkonto ist für das Medical Center in Merced im US-Bundesstaat Kalifornien gedacht.

Die Betrüger forderten zunächst einen Geldbetrag von 440.000 US-Dollar per Fax an. Ihre Anforderungen legitimierten sie mit der Unterschrift des Präsidenten der Stiftung. Diese hatten sie ausgerechnet von der Webseite der Stiftung selbst. Dort waren mehrere Dokumente verfügbar, die die Unterschrift enthielten.

Das Konto, auf das Wells Fargo das Geld überweisen sollte, gab es aber nicht. Möglicherweise wollten die Betrüger zunächst prüfen, ob ihr Scam überhaupt funktioniert. Wells Fargo kontaktierte den anonymen Betrüger, um die Kontonummer zu verifizieren. Auch eine zweite Überweisung klappte jedoch nicht. Erst Monate und mehrere Anfragen später schaffte es das Geldinstitut, etwa 1 Million US-Dollar auf ein tatsächlich vorhandenes Konto in Hongkong zu überweisen. Nach einer weiteren Anfrage transferierte Wells Fargo ein weiteres Mal etwa 1,1 Millionen US-Dollar. Erst, als Betrüger abermals 2,3 Millionen US-Dollar anforderten, schöpfte das Geldinstitut Verdacht. Es erstattete das fälschlich überwiesene Geld an die Stiftung zurück und Anzeige gegen unbekannt.

Der Klassiker: Industriespionage

Industriespionage gehört mit zu den ältesten und erfolgreichsten Maschen des Social Engineerings. Als legitim betrachtete Mitarbeiter können sich Zugang zu den geheimsten Labors verschaffen und Konkurrenten ausspionieren. Jüngst will die britische Staubsaugerfirma Dyson einen Spion von Bosch bei sich entdeckt haben, der dort

Geschäftsgeheimnisse gesammelt und an die deutsche Firma Bosch weitergeben haben soll. Der Mitarbeiter, dessen Identität noch unbekannt ist, soll zwei Jahre lang in Dysons Entwicklungsabteilung für elektrische Motoren gearbeitet haben.

Die Abteilung ist laut Dyson in einem Gebäudetrakt mit höchster Sicherheit untergebracht, der Zugang nur per Fingerabdruckerkennung möglich. Bosch weist die Vorwürfe zurück. Der ehemalige Mitarbeiter habe bei Bosch in der Abteilung für Gartengeräte gearbeitet. Dyson hat gegen Bosch Klage vor einem britischen Gericht eingereicht.

Schon früher wurden deutsche Firmen beschuldigt, bei britischen Unternehmen abgekupfert zu haben. Im späten 19. Jahrhundert hatte Großbritannien einen derart großen Vorsprung bei Qualitätsprodukten vor dem Nachzügler auf dem Kontinent, dass reihenweise deutsche Facharbeiter zum "Anlernen" auf die Insel geschickt wurden. Damit die immer noch minderwertigen und fast identischen deutschen Produkte von den britischen Originalen zu unterscheiden waren, setzte Großbritannien damals die Bezeichnung "Made in Germany" durch.

...und eine ganze Brücke

Einer der Basistricks bei Social Engineering sind gefälschte Dokumente. Mit diesen konnten Diebe in der Nähe von Slavkov in Tschechien einen ganzen Fußgängerübergang abbauen und die darunterliegenden Bahngleise gleich mit. Die Metalldiebe rückten dafür sogar mit einem Kran an. Als die örtliche Polizei nach dem Rechten sehen wollte, präsentierten die Diebe offensichtlich gut gefälschte Genehmigungspapiere. Sie seien mit dem Abriss beauftragt worden, um Platz für einen neuen Fahrradweg zu machen.

Erst nachdem die Brücke verschwunden war, überprüften Mitarbeiter der örtlichen Bahnstation den vermeintlichen Auftrag. Angaben über die Höhe des Verlusts reichen von mehreren Tausend Euro an Materialkosten bis hin zu mehreren Millionen Euro für den Wiederaufbau der entwendeten Brücke. Die Gleisstrecke war aber laut Bahn bereits stillgelegt.

Metallabbau hat in der Gegend um Slavkov Tradition: Bereits im 2. Jahrtausend vor Christus wurde dort Zinnab- gebaut, die Region war bis ins 16. Jahrhundert für das Metall berühmt. Es wurde beispielsweise von der Familie Fugger aus Augsburg gehandelt.

Betrug ist nicht Hacken

Auch wenn sich einige Diebe wie im Fall des IT-Journalisten Honan selbst gerne Hacker nennen, verstoßen sie gegen die allgemein anerkannte Ethik, dass persönliche Daten geschützt werden müssen. Betrug durch Social Engineering hat nichts mit Hacking zu tun und kann auch furchtbare Konsequenzen für die Opfer haben. Das zeigt auch der tragische Fall der britischen Krankenschwester.

Sie war auf einen Trickanruf von zwei Radiomoderatoren hereingefallen, die sich als Queen Elisabeth II und Prince

Charles ausgaben und Informationen über den Gesundheitszustand der schwangeren Herzogin Kate erbaten. Obwohl sie lediglich den Anruf durchgestellt hatte, beging die Krankenschwester Selbstmord, nachdem der Sender die so erschlichenen Informationen veröffentlicht hatte. Dem Sender wurden schwere Vorwürfe gemacht, weil er das Opfer nicht aufgeklärt und den Telefonscherz ohne dessen Erlaubnis veröffentlicht hatte.

Conheady hat viel Verständnis für die Opfer von Social Engineering, auch für ihre eigenen. Denn ihre Aufgabe ist es, mit Social-Engineering-Tricks in Unternehmen einzudringen und so Sicherheitslücken aufzudecken. Mitarbeiter, die auf Conheadys Tricks hereinfallen, werden meist aufgeklärt, aber nicht gescholten. Sie könne ihren Job ohne Mitgefühl oder Empathie für ihre potenziellen Opfer gar nicht machen, sagt sie. Sie müsse sich ja in diese Personen hineinversetzen können, um Wege zu finden, sie zu überlisten.

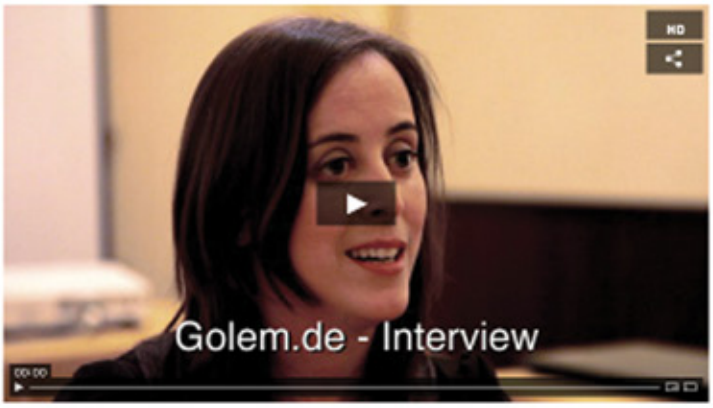
Nicht nur für die Opfer, auch für die Scammer selbst kann Betrug durch Social Engineering schwere Folgen haben. Das zeigt ein Fall in den USA. Dort wurde der selbsternannte Paparazzi-Hacker zu zehn Jahren Haft verurteilt. Er hatte prominente Opfer wie Scarlett Johansson jahrelang ausspioniert, deren private Daten veröffentlicht und damit geprahlt.

2012

Die Verschwindetricks der Social Engineers

Per Social Engineering ist es Betrügern 2012 gelungen, die gesamte digitale Identität eines Wired-Journalisten verschwinden zu lassen. Im Real Life ließen sie sogar eine ganze Brücke mitgehen.

Jenseits von Phishing-Attacken, als Nacktfotos getarnter Malware im E-Mail-Postfach oder sprachlich unbeholfenen Aufforderungen, bei lukrativen Finanztransaktionen in Nigeria behilflich zu sein, gibt es Betrugsmaschen, auf die selbst Polizei und IT-Experten hereinfallen: Hacks auf Onlinekonten, Identitätsklau, Industriespionage, Diebstahl mit digitalen Unterschriften oder mit gefälschten Dokumenten. Die Social-Engineering-Expertin und Sicherheitsprüferin Sharon Conheady hat auf der Deepsec 2012 die spektakulärsten Scams 2012 präsentiert.



Video: Interview Sharon Conheady über Social Engineering (10:41)

Gesamtes digitales Leben gelöscht

Das komplette digitale Leben des Wired-Journalisten Matt Honan wurde von Angreifern gelöscht. Sie verschafften sich durch Social Engineering genügend Informationen, um sich bei einem Anruf beim Apple-Support als Honan zu authentifizieren und forderten ein neues Passwort für Honans Me.com-Account an. Damit ausgestattet, konnten sie gleich auch Honans Apple-ID ändern. Zuvor hatten sie noch die Bestätigungs-E-Mail in den Papierkorb verschoben. Kurz darauf setzten sie sein Gmail-Passwort und die Zugangsdaten zu seinem Konto bei Google zurück.

Kleinlaut musste Honan zugeben, dass es ein Fehler gewesen war, sämtliche E-Mail-Konten mit dem gleichen Namen zu versehen und sie auch mit verschiedenen Konten zu verknüpfen. Backups hatte er nicht. Hätte er seinen Google-Account mit zweifacher Authentifizierung abgesichert, wären die Hacker nicht weitergekommen, schreibt er in einem ausführlichen Bericht. Er kritisierte aber auch Apple, das mit

Verschwindetrick auf traditionelle Art (Bild: George W. Hales/Getty Images)

Artikel: 2012 Die Verschwindetricks der Social Engineers

Inhalt:
- Ziel der Scammer war das Twitter-Konto
- Falscher Paul Allen verschafft sich Kontozugang
- Der Klassiker: Industriespionage
- Betrug ist nicht Hacken

Datum: 26.12.2012, 09:25

Autor: Jörg Thoma

Themen: Security, Deepsec, Hacker, Malware, Paul Allen, iCloud, Internet, Politik/Recht

nur wenigen Informationen das Zurücksetzen eines Passworts erlaubt.

Ziel der Scammer war das Twitter-Konto

Auch das Passwort für Honans Twitter-Account forderten die Hacker an und verbreiteten darüber rassistische Tweets. Über den iCloud-Account setzten sie iPhone, iPad und Macbook zurück und löschten schließlich auch sein Google-Konto. E-Mails, Familienfotos, alles sei weg, beklagt Honan. Die Angreifer hatten es zwar nur auf sein Twitter-Konto abgesehen, löschten aber alles andere, damit Honan ihn nicht wieder zurückbekommen würde.

Letztendlich benötigt Apple nur die Rechnungsadresse und die letzten vier Zahlen der Kreditkarte, um einen Zugang zurückzusetzen, wie das Unternehmen auf Anfrage von Wired bestätigte. Wie die Betrüger daran gekommen waren, erfuhr Honan später von ihnen selbst. Sie tauschten sich über Honans neuen Twitter-Account aus.

Erst Amazon-, dann Google- und Apple-Konten

Honans Rechnungsadresse erfuhren die Hacker durch einen einfachen Whois-Lookup seiner privaten Domäne. Genauso gut hätten sie aber öffentliche Verzeichnisse im Internet durchforsten können, schreibt Honan. Den wiederkehrenden Namen "mhonan" in seinen diversen E-Mail-Adressen erfuhren sie über seinen Twitter-Account.

Die benötigten Ziffern seiner Kreditkartennummer holten sich die Hacker bei Amazon. Dort hatte Honan ebenfalls ein Konto. Zunächst riefen die Betrüger beim Support an und gaben die Rechnungsadresse, die E-Mail-Adresse und den Namen an. Nach erfolgreicher Authentifizierung verlangten sie, dem Konto eine zweite Kreditkartennummer hinzuzufügen, und gaben eine - natürlich gefälschte - Nummer durch.

Später riefen sie nochmals dort an, gaben an, keinen Zugang zum Konto mehr zu haben und gaben wieder Rechnungsadresse, Name, E-Mail-Adresse und die neue Kreditkartennummer an. Daraufhin konnten sie dem Konto eine zweite E-Mail-Adresse hinzufügen, an die dann ein neues Passwort versendet wurde. Damit ausgestattet, loggten sie sich ein und erfuhren die Ziffern, die sie für die Authentifizierung bei Apple benötigten.

Es war nicht persönlich gemeint

Sie hätten es nicht auf ihn persönlich abgesehen, schrieb ihm einer der Betrüger später. Sie hätten nur sein Twitter-Konto kapern wollen. Es hätte schlimmer kommen können, schrieb der zerknirschte Journalist, denn er habe zahlreiche einflussreiche Namen in seiner Kontaktliste, die ebenfalls hätten angegriffen werden können. Er trauere aber um die unwiederbringlich gelöschten Fotos seiner Familie, vor allem seiner kleinen Tochter, die er seit ihrer Geburt gesammelt hatte. Auch sein Ruf als IT-Journalist habe gelitten.

Dem Hacker habe sein Tun später leidgetan, schreibt Honan. Nicht er, sondern sein Kumpel habe Honans Daten gelöscht, teilte der Angreifer mit. Auf die Frage Honans, warum er den Hack eigentlich durchgeführt habe, antwortete er lapidar, er wolle auf die Schwachstelle hinweisen. Die Hackerethik besagt allerdings, dass öffentliche Daten genutzt und private Daten geschützt werden müssen.

Verschwindetrick auf traditionelle Art (Bild: George W. Hales/Getty Images)

Artikel: 2012 Die Verschwindetricks der Social Engineers

Inhalt:
- Ziel der Scammer war das Twitter-Konto
- Falscher Paul Allen verschafft sich Kontozugang
- Der Klassiker: Industriespionage
- Betrug ist nicht Hacken

Datum: 26.12.2012, 09:25

Autor: Jörg Thoma

Themen: Security, Deepsec, Hacker, Malware, Paul Allen, iCloud, Internet, Politik/Recht

Falscher Paul Allen verschafft sich Kontozugang

Stars oder Millionäre sind natürlich ein beliebtes Angriffsziel für Scammer, da über sie viel bekannt ist und das Hacken eine medienwirksame Aktion bedeutet - oder einfach, weil sie viel Geld haben.

Nicht besonders geschickt hat sich ein unerlaubt abwesender US-Soldat in den USA angestellt, der sich zunächst erfolgreich als der Millionär und Microsoft-Mitbegründer Paul Allen ausgab. Er rief bei Allens Bank an und erklärte, dass er seine Bankkarte daheim verlegt hätte. Er wolle die Karte zwar nicht als verloren melden, hätte aber gerne sobald wie möglich eine zweite. Der Citibank-Mitarbeiter war offensichtlich so hilfsbereit, dass er eine zusätzliche Adresse aufnahm, an die er die zweite Karte per Express rausschickte. Der US-Soldat gab auch gleich seine Telefonnummer an.

Viel Erfolg hatte der Soldat aber nicht. Ihm gelang zwar zunächst eine Überweisung in Höhe von etwa 600 US-Dollar mit der neuen Karte, eine zweite Überweisung in Höhe von 15.000 US-Dollar sowie Einkäufe in einem Computerspielgeschäft fielen aber der Betrugsabteilung in der Bank auf. Der Soldat wurde verhaftet und angeklagt. Wie der Betrüger den Bankmitarbeiter dazu überredete, die zweite Karte auszustellen, bleibt ein Geheimnis. Die Bank gab dazu keinen Kommentar ab.

Mit öffentlicher Unterschrift zu Millionen

Gleich mehrere Anläufe benötigten Scammer aus Hongkong, um etwa 2 Millionen US-Dollar zu erbeuten. Das Geld ergaunerten sie von Wells Fargo, das ein gemeinsames Treuhandkonto des US-Bezirks Merced und der Catholic Healthcare West verwaltet. Das Geld auf dem Treuhandkonto ist für das Medical Center in Merced im US-Bundesstaat Kalifornien gedacht.

Die Betrüger forderten zunächst einen Geldbetrag von 440.000 US-Dollar per Fax an. Ihre Anforderungen legitimierten sie mit der Unterschrift des Präsidenten der Stiftung. Diese hatten sie ausgerechnet von der Webseite der Stiftung selbst. Dort waren mehrere Dokumente verfügbar, die die Unterschrift enthielten.

Das Konto, auf das Wells Fargo das Geld überweisen sollte, gab es aber nicht. Möglicherweise wollten die Betrüger zunächst prüfen, ob ihr Scam überhaupt funktioniert. Wells Fargo kontaktierte den anonymen Betrüger, um die Kontonummer zu verifizieren. Auch eine zweite Überweisung klappte jedoch nicht. Erst Monate und mehrere Anfragen später schaffte es das Geldinstitut, etwa 1 Million US-Dollar auf ein tatsächlich vorhandenes Konto in Hongkong zu überweisen. Nach einer weiteren Anfrage transferierte Wells Fargo ein weiteres Mal etwa 1,1 Millionen US-Dollar. Erst, als Betrüger abermals 2,3 Millionen US-Dollar anforderten, schöpfte das Geldinstitut Verdacht. Es erstattete das fälschlich überwiesene Geld an die Stiftung zurück und Anzeige gegen unbekannt.

‹ 1 2 3 4 5 ›

Verschwindetrick auf traditionelle Art (Bild: George W. Hales/Getty Images)

Artikel: 2012
Die Verschwindetricks der Social Engineers

Inhalt:
- Ziel der Scammer war das Twitter-Konto
- Falscher Paul Allen verschafft sich Kontozugang
- Der Klassiker: Industriespionage
- Betrug ist nicht Hacken

Datum: 26.12.2012, 09:25

Autor: Jörg Thoma

Themen: Security, Deepsec, Hacker, Malware, Paul Allen, iCloud, Internet, Politik/Recht

Der Klassiker: Industriespionage

Industriespionage gehört mit zu den ältesten und erfolgreichsten Maschen des Social Engineerings. Als legitim betrachtete Mitarbeiter können sich Zugang zu den geheimsten Labors verschaffen und Konkurrenten ausspionieren. Jüngst will die britische Staubsaugerfirma Dyson einen Spion von Bosch bei sich entdeckt haben, der dort Geschäftsgeheimnisse gesammelt und an die deutsche Firma Bosch weitergeben haben soll. Der Mitarbeiter, dessen Identität noch unbekannt ist, soll zwei Jahre lang in Dysons Entwicklungsabteilung für elektrische Motoren gearbeitet haben.

Die Abteilung ist laut Dyson in einem Gebäudetrakt mit höchster Sicherheit untergebracht, der Zugang nur per Fingerabdruckerkennung möglich. Bosch weist die Vorwürfe zurück. Der ehemalige Mitarbeiter habe bei Bosch in der Abteilung für Gartengeräte gearbeitet. Dyson hat gegen Bosch Klage vor einem britischen Gericht eingereicht.

Schon früher wurden deutsche Firmen beschuldigt, bei britischen Unternehmen abgekupfert zu haben. Im späten 19. Jahrhundert hatte Großbritannien einen derart großen Vorsprung bei Qualitätsprodukten vor dem Nachzügler auf dem Kontinent, dass reihenweise deutsche Facharbeiter zum "Anlernen" auf die Insel geschickt wurden. Damit die immer noch minderwertigen und fast identischen deutschen Produkte von den britischen Originalen zu unterscheiden waren, setzte Großbritannien damals die Bezeichnung "Made in Germany" durch.

...und eine ganze Brücke

Einer der Basistricks bei Social Engineering sind gefälschte Dokumente. Mit diesen konnten Diebe in der Nähe von Slavkov in Tschechien einen ganzen Fußgängerübergang abbauen und die darunterliegenden Bahngleise gleich mit. Die Metalldiebe rückten dafür sogar mit einem Kran an. Als die örtliche Polizei nach dem Rechten sehen wollte, präsentierten die Diebe offensichtlich gut gefälschte Genehmigungspapiere. Sie seien mit dem Abriss beauftragt worden, um Platz für einen neuen Fahrradweg zu machen.

Erst nachdem die Brücke verschwunden war, überprüften Mitarbeiter der örtlichen Bahnstation den vermeintlichen Auftrag. Angaben über die Höhe des Verlusts reichen von mehreren Tausend Euro an Materialkosten bis hin zu mehreren Millionen Euro für den Wiederaufbau der entwendeten Brücke. Die Gleisstrecke war aber laut Bahn bereits stillgelegt.

Metallabbau hat in der Gegend um Slavkov Tradition: Bereits im 2. Jahrtausend vor Christus wurde dort Zinn abgebaut, die Region war bis ins 16. Jahrhundert für das Metall berühmt. Es wurde beispielsweise von der Familie Fugger aus Augsburg gehandelt.

‹ 1 2 3 4 5 ›

Verschwindetrick auf traditionelle Art (Bild: George W. Hales/Getty Images)

Datum: 26.12.2012, 09:25

Autor: Jörg Thoma

Themen: Security, Deepsec, Hacker, Malware, Paul Allen, iCloud, Internet, Politik/Recht

Betrug ist nicht Hacken

Auch wenn sich einige Diebe wie im Fall des IT-Journalisten Honan selbst gerne Hacker nennen, verstoßen sie gegen die allgemein anerkannte Ethik, dass persönliche Daten geschützt werden müssen. Betrug durch Social Engineering hat nichts mit Hacking zu tun und kann auch furchtbare Konsequenzen für die Opfer haben. Das zeigt auch der tragische Fall der britischen Krankenschwester.

Sie war auf einen Trickanruf von zwei Radiomoderatoren hereingefallen, die sich als Queen Elisabeth II und Prince Charles ausgaben und Informationen über den Gesundheitszustand der schwangeren Herzogin Kate erbaten. Obwohl sie lediglich den Anruf durchgestellt hatte, beging die Krankenschwester Selbstmord, nachdem der Sender die so erschlichenen Informationen veröffentlicht hatte. Dem Sender wurden schwere Vorwürfe gemacht, weil er das Opfer nicht aufgeklärt und den Telefonscherz ohne dessen Erlaubnis veröffentlicht hatte.

Conheady hat viel Verständnis für die Opfer von Social Engineering, auch für ihre eigenen. Denn ihre Aufgabe ist es, mit Social-Engineering-Tricks in Unternehmen einzudringen und so Sicherheitslücken aufzudecken. Mitarbeiter, die auf Conheadys Tricks hereinfallen, werden meist aufgeklärt, aber nicht gescholten. Sie könne ihren Job ohne Mitgefühl oder Empathie für ihre potenziellen Opfer gar nicht machen, sagt sie. Sie müsse sich ja in diese Personen hineinversetzen können, um Wege zu finden, sie zu überlisten.

Nicht nur für die Opfer, auch für die Scammer selbst kann Betrug durch Social Engineering schwere Folgen haben. Das zeigt ein Fall in den USA. Dort wurde der selbsternannte Paparazzi-Hacker zu zehn Jahren Haft verurteilt. Er hatte prominente Opfer wie Scarlett Johansson jahrelang ausspioniert, deren private Daten veröffentlicht und damit geprahlt. •

‹ 1 2 3 4 5

‹ Der Klassiker: Industriespionage

Verschwindetrick auf traditionelle Art (Bild: George W. Hales/Getty Images)

Artikel: 2012
Die Verschwindetricks der Social Engineers

Inhalt:
- Ziel der Scammer war das Twitter-Konto
- Falscher Paul Allen verschafft sich Kontozugang
- Der Klassiker: Industriespionage
- Betrug ist nicht Hacken

Datum: 26.12.2012, 09:25

Autor: Jörg Thoma

Themen: Security, Deepsec, Hacker, Malware, Paul Allen, iCloud, Internet, Politik/Recht

http://oe1.orf.at/programm/322335

matrix - computer & neue medien

Datum: 09. 12. 2012

Autor: Sarah Kriesche

Löcher im Netz. Die DeepSec 2012

Die Sicherheitskonferenz DeepSec findet in diesem Jahr bereits zum 6. Mal statt. Die heurige Veranstaltung widmet sich den Schwerpunkten "Cyberwar", mobile Geräte und Infrastruktur. Nicht nur das Fachpublikum, sondern auch die Endverbraucher sollen auf dieser Veranstaltung, die längst internationale Beachtung gefunden hat, für die Bedeutung sicherer Netzwerke und ein sicheres Internet sensibilisiert werden. Sarah Kriesche berichtet über die Bedrohungen aus dem Netz.

zur Sendereihe

Standort: oe1.ORF.at

OE1 ORF.at

Navigation

matrix - computer & neue medien

Sonntag
09. Dezember 2012
22:30

Löcher im Netz. Die DeepSec 2012. Gestaltung: Sarah Kriesche

Die Sicherheitskonferenz DeepSec findet in diesem Jahr bereits zum 6. Mal statt. Die heurige Veranstaltung widmet sich den Schwerpunkten "Cyberwar", mobile Geräte und Infrastruktur. Nicht nur das Fachpublikum, sondern auch die Endverbraucher sollen auf dieser Veranstaltung, die längst internationale Beachtung gefunden hat, für die Bedeutung sicherer Netzwerke und ein sicheres Internet sensibilisiert werden. Sarah Kriesche berichtet über die Bedrohungen aus dem Netz.

zurück

zur Sendereihe

Kategorie: Wissen

Programm

Mo	Di	Mi	Do	Fr	Sa	So
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16

http://fm4.orf.at/radio/stories/1708743

Connected (13-17)

mit Nina Hofer

Merry Clipmas! Der FM4 Video-Advent-Kalender

Datum: 01.12.2012

Autor: Sarah Kriesche

Deep Sec

Sicherheitskonferenz in Wien, Rückschau, IT ; Aufhänger ist der Hoax um eine Facebook-Gold-Mitgliedschaft, die es natürlich nicht gibt, und wie leicht man an Geld und Daten von leichtgläubigen Social Media Noobs kommt. (Sarah Kriesche)

Trauma

Eine junge Frau wacht nach einem Autounfall im Krankenhaus auf und versucht sich zu erinnern. In Form von Bildern und Photos reflektiert sie über ihr Leben. Der/die SpielerIn klickt sich durch eine menschenleere Welt, auf der Suche nach Hinweisen. Die Bilder von verlassenen Kölner Orten bei Nacht, dazu ein sphärischer Soundtrack und die unheimliche Erzählstimme der jungen Frau saugen einen in die melancholische Welt von „Trauma“, das eigentlich nur mehr als Computerspiel bezeichnet werden kann, weil es noch keinen besseren Begriff dafür gibt. Conny Lee hat die interaktiven Bilder von Trauma erforscht.

Cribs

In ihrer Heimat England sind sie die DIY-Vorzeigeband, die regelmässig Konzerte ausverkauft und heuer auch mit dem Q Magazin Spirit Of Independence Award ausgezeichnet wurde. Im Fm4 Blinddate mit Susi Ondrusova sprechen Ross Jarman und Gary Jarman u.a. über Queen, Beat Happening, Steve Albini und Beth Ditto.

Artist Of The Week: Interpol (Arthur Einöder) | Crystal Castles (Dani Derntl) |

Amadou & Mariam (Eva Umbauer) | Linus Volkmann - Kein Schlaf bis Langenselbold (David Pfister)

Connected (13-17)

mit Nina Hofer

Merry Clipmas! Der FM4 Video-Advent-Kalender

Deep Sec (https://deepsec.net/)
Sicherheitskonferenz in Wien, Rückschau, IT ; Aufhänger ist der Hoax um eine Facebook-Gold-Mitgliedschaft, die es natürlich nicht gibt, und wie leicht man an Geld und Daten von leichtgläubigen Social Media Noobs kommt. (Sarah Kriesche)

Trauma
Eine junge Frau wacht nach einem Autounfall im Krankenhaus auf und versucht sich zu erinnern. In Form von Bildern und Photos reflektiert sie über ihr Leben. Der/die SpielerIn klickt sich durch eine menschenleere Welt, auf der Suche nach Hinweisen. Die Bilder von verlassenen Kölner Orten bei Nacht, dazu ein sphärischer Soundtrack und die unheimliche Erzählstimme der jungen Frau saugen einen in die melancholische Welt von „Trauma“, das eigentlich nur mehr als Computerspiel bezeichnet werden kann, weil es noch keinen besseren Begriff dafür gibt. Conny Lee hat die interaktiven Bilder von Trauma erforscht.

Cribs (http://www.thecribs.com/official/)
In ihrer Heimat England sind sie die DIY-Vorzeigeband, die regelmässig Konzerte ausverkauft und heuer auch mit dem Q Magazin Spirit Of Independence Award (http://www.youtube.com/watch?v=4tHizgTRBAg) ausgezeichnet wurde. Im Fm4 Blinddate mit Susi Ondrusova sprechen Ross Jarman und Gary Jarman u.a. über Queen, Beat Happening, Steve Albini und Beth Ditto.

Artist Of The Week (/artistoftheweek) : Interpol (Arthur Einöder) | Crystal Castles (http://www.crystalcastles.com/) (Dani Derntl) |
Amadou & Mariam (http://www.amadou-mariam.com/?utm_source=Email+Campaign&utm_medium=email&utm_campaign=188866-Amadou+and+Mariam+) (Eva Umbauer) | Linus Volkmann - Kein Schlaf bis Langenselbold (David Pfister)

http://www.golem.de/news/vmware-esxi-5-uebernahme-des-hypervisors-ueber-ein-gastsystem-1211-96059.html

VMWARE ESXI 5

Übernahme des Hypervisors über ein Gastsystem

Datum: 30.11.2012

Autor:Jörg Thoma

Deepsec 2012 Mit modifizierter Firmware können Hacker mit einer Root-Shell auf den ESXi-5-Hypervisor von VMware zugreifen. Das haben die beiden Sicherheitsexperten Pascal Turbing und Hendrik Schmidt auf der Deepsec 2012 demonstriert.

Ohne großen Aufwand können Angreifer auf den Hypervisor von VMware zugreifen. Sie können dazu weitgehend unbekannte Parameter in den Beschreibungsdateien der virtuellen Festplatten für Gastsysteme nutzen, um sich schreibenden Zugriff auf das Root-Dateisystem des Hypervisors zu verschaffen. Da der Zugriff auf die virtuelle Infrastruktur in entfernten Systemen weitgehend vom Provider ungeprüft erfolgt, werten die Sicherheitsexperten Pascal Turbing und Hendrik Schmidt diese Lücke als gravierend. Sie demonstrierten auf der Deepsec 2012 erstmals auch einen Zugriff auf den Hypervisor mit einer Root-Shell.

Zunächst fiel den Sicherheitsexperten auf, dass sie mit eigenen Parametern im Abschnitt Disk Descriptor aus Gastsystemen heraus auf die Lodgdateien des Hypervisors zugreifen können. Dazu reicht beispielsweise der Eintrag VMFS "/scratch/log/vmkernel1.0.gz". Danach kann die Logdatei als Loopback-Device mit dem Befehl losetup in das Linux-Gastsystem eingebunden werden.

Erst Logdateien, dann ganze Verzeichnisse

Turbing und Schmidt gingen noch ein Schritt weiter. Mit dem Zugriff auf die Logdateien ließen sich auch weitere Informationen der virtuellen Umgebung auslesen, etwa der Name der von dem Hypervisor verwendeten Festplatten. Diese konnten sie dann mit dem Konfigurationseintrag RW 0 VMFSRAW "/dev/disk/Diskname" ebenfalls ins Gastsystem einbinden.

Das funktioniert auch deshalb, weil Linux Geräte als Dateien behandelt. Das Einbinden einzelner Verzeichnisse ist ebenfalls möglich. Lediglich Dateien in der Ramdisk des Hypervisors konnten sie zunächst nicht einbinden, denn sie wird dynamisch während des Starts des Hypervisors erzeugt und mit den Parametern aus der Bootbank-Partition gefüttert, aus der das Root-Dateisystem des Hypervisors generiert wird.

Zugriff auf die Konfigurationsdateien des Hypervisors

Also galt es, Zugriff auf das Bootbank-Verzeichnis zu erhalten. Es wurde wie bereits erwähnt mit Schreibzugriff im Gastsystem eingebunden. Die dort abgelegten Dateien sind mit einem speziellen Tar-Gz-Format gepackt. Sie können nur mit der Binärdatei Vmtar und der Bibliothek Libvmlibs.so erstellt werden, die jeder VMware-Installation beiliegen und in das Gastsystem kopiert werden können.

Die Hacker konnten so eine modifizierte Firewall-Konfigurationsdatei im Bootbank-Verzeichnis ablegen und beispielsweise per DoS-Angriff einen Neustart des Hypervisors erzwingen. Danach konnte sie sich in die Shell des Hypervisors einloggen.

Unbefugte Nutzer fernhalten

Ein solcher Angriff kann unter folgenden Voraussetzungen erfolgen: Das präparierte Gastsystem muss über das von VMware bereitgestellte API ohne Änderungen oder Verifizierung auf das System mit dem Hypervisor ESXi 5 übertragen werden. Die Dateien des Gastsystems müssen auf einer eigenständigen Partition liegen, die nicht vom Hypervisor genutzt wird.

Bislang weist der VMware-Hersteller lediglich darauf hin, dass grundsätzlich Unbefugten kein Zugang zum Hypervisor gewährt werden sollte. Von den vier kontaktierten Serviceprovidern, die virtuelle Umgebungen mit ESXi 5 anbieten, geben nur zwei an, die auf ihre Server hochgeladenen Dateien zu prüfen, sagten Turbing und Schmidt zu Golem.de.

Eine genaue Beschreibung des Angriffsvektors haben die Hacker in ihrem Blog veröffentlicht.

VMWARE ESXI 5

Übernahme des Hypervisors über ein Gastsystem

Deepsec 2012 Mit modifizierter Firmware können Hacker mit einer Root-Shell auf den ESXi-5-Hypervisor von VMware zugreifen. Das haben die beiden Sicherheitsexperten Pascal Turbing und Hendrik Schmidt auf der Deepsec 2012 demonstriert.

Die Hacker Pascal Turbing und Hendrik Schmidt demonstrierten die Übernahme des ESXi-Hypervisors von VMware. (Bild: Andreas Sebayang/Golem.de)

Datum: 30.11.2012, 12:09
Autor: Jörg Thoma
Themen: Deepsec, Cloud Computing, Dateisystem, Server-Applikationen, VMware, Virtualisierung, API, Server, Applikationen, Security

Ohne großen Aufwand können Angreifer auf den Hypervisor von VMware zugreifen. Sie können dazu weitgehend unbekannte Parameter in den Beschreibungsdateien der virtuellen Festplatten für Gastsysteme nutzen, um sich schreibenden Zugriff auf das Root-Dateisystem des Hypervisors zu verschaffen. Da der Zugriff auf die virtuelle Infrastruktur in entfernten Systemen weitgehend vom Provider ungeprüft erfolgt, werten die Sicherheitsexperten Pascal Turbing und Hendrik Schmidt diese Lücke als gravierend. Sie demonstrierten auf der Deepsec 2012 erstmals auch einen Zugriff auf den Hypervisor mit einer Root-Shell.

Zunächst fiel den Sicherheitsexperten auf, dass sie mit eigenen Parametern im Abschnitt *Disk Descriptor* aus Gastsystemen heraus auf die Lodgdateien des Hypervisors zugreifen können. Dazu reicht beispielsweise der Eintrag *VMFS "/scratch/log/vmkernel1.0.gz"*. Danach kann die Logdatei als Loopback-Device mit dem Befehl *losetup* in das Linux-Gastsystem eingebunden werden.

Erst Logdateien, dann ganze Verzeichnisse

Turbing und Schmidt gingen noch ein Schritt weiter. Mit dem Zugriff auf die Logdateien ließen sich auch weitere Informationen der virtuellen Umgebung auslesen, etwa der Name der von dem Hypervisor verwendeten Festplatten. Diese konnten sie dann mit dem Konfigurationseintrag *RW 0 VMFSRAW "/dev/disk/Diskname"* ebenfalls ins Gastsystem einbinden.

Das funktioniert auch deshalb, weil Linux Geräte als Dateien behandelt. Das Einbinden einzelner Verzeichnisse ist ebenfalls möglich. Lediglich Dateien in der Ramdisk des Hypervisors konnten sie zunächst nicht einbinden, denn sie wird dynamisch während des Starts des Hypervisors erzeugt und mit den Parametern aus der Bootbank-Partition gefüttert, aus der das Root-Dateisystem des Hypervisors generiert wird.

Zugriff auf die Konfigurationsdateien des Hypervisors

Also galt es, Zugriff auf das Bootbank-Verzeichnis zu erhalten. Es wurde wie bereits erwähnt mit Schreibzugriff im Gastsystem eingebunden. Die dort abgelegten Dateien sind mit einem speziellen Tar-Gz-Format gepackt. Sie können nur mit der Binärdatei Vmtar und der Bibliothek Libvmlibs.so erstellt werden, die jeder VMware-Installation beiliegen und in das Gastsystem kopiert werden können.

Die Hacker konnten so eine modifizierte Firewall-Konfigurationsdatei im Bootbank-Verzeichnis ablegen und beispielsweise per DoS-Angriff einen Neustart des Hypervisors erzwingen. Danach konnte sie sich in die Shell des Hypervisors einloggen.

Unbefugte Nutzer fernhalten

Ein solcher Angriff kann unter folgenden Voraussetzungen erfolgen: Das präparierte Gastsystem muss über das von VMware bereitgestellte API ohne Änderungen oder Verifizierung auf das System mit dem Hypervisor ESXi 5 übertragen werden. Die Dateien des Gastsystems müssen auf einer eigenständigen Partition liegen, die nicht vom Hypervisor genutzt wird.

Bislang weist der VMware-Hersteller lediglich darauf hin, dass grundsätzlich Unbefugten kein Zugang zum Hypervisor gewährt werden sollte. Von den vier kontaktierten Serviceprovidern, die virtuelle Umgebungen mit ESXi 5 anbieten, geben nur zwei an, die auf ihre Server hochgeladenen Dateien zu prüfen, sagten Turbing und Schmidt zu Golem.de.

Eine genaue Beschreibung des Angriffsvektors haben die Hacker in ihrem Blog veröffentlicht. •

http://www.golem.de/news/snoop-it-fuer-ios-sicherheitschecks-von-iphone-apps-fuer-fast-jeden-moeglich-1211-96034.html

SNOOP-IT FÜR IOS

Sicherheitschecks von iPhone-Apps für fast jeden möglich

Datum:29.11.2012

Autor:Andreas Sebayang

Deepsec 2012 Die Snoop-It-App soll jedem eine Basisüberprüfung der Sicherheit von Apps ermöglichen. Das könnte dazu führen, dass viele iOS-Entwickler entdeckt werden, die auf fragwürdige Art und Weise Daten erheben.

Andreas Kurtz von den NESO Security Labs und der Universität Erlangen-Nürnberg arbeitet an einem einfach zu bedienenden Werkzeug, um iOS-Anwendungen auf ihre Sicherheit hin zu überprüfen. Die Snoop-It-App wird auf einem iPhone oder iPad installiert und dort über einen simplen Dialog konfiguriert. Kurtz demonstrierte die Anwendung, die sich noch in einem Vorversionsstatus befindet, auf der Deepsec in Wien. Dabei fiel auf, dass sie vergleichsweise einfach zu bedienen ist. Das Herumhacken auf der Kommandozeile ist nicht einmal notwendig. Stattdessen nutzt der Anwender einfach einen Browser und verbindet sich mit der Snoop-It-App, die gerade eine App untersucht.

Snoop-It-Demo

Über den Browser kann dann mit den Sicherheitstests begonnen werden. Einige dieser Tests sind sehr einfach gehalten. So ist es etwa möglich, der App einen anderen Ort vorzugaukeln. Die Auswahl geschieht über Google Maps. Interessant ist das, um etwa eine Kontrolle von Apps zu ermöglichen, die nur in bestimmten Arealen, etwa dem Firmengelände, benutzt werden dürfen. Auch der Netzwerkverkehr kann untersucht werden. So sieht der Anwender, ob und wie die App auf externe Server zugreift und erhobene Daten abliefert und ob dies verschlüsselt geschieht. Zugriffe auf Systemkomponenten (Schlüsselbund, Dateien, Kontakte und Fotos) werden ebenfalls aufgenommen.

Mit Hilfe eines Ampelsystems werden kritische Zugriffe außerdem schnell erfassbar gemacht. Zudem kann der Anwender Hardware-IDs (MACs und UDID) fälschen, um zu sehen, wie die App darauf reagiert. Bekanntlich nutzen einige Apps, darunter auch das populäre Whatsapp, diese als feste Passwörter.

Potenzial für eine umfassende Sicherheitsüberprüfung des App-Katalogs

Die Snoop-It-App hat das Potenzial, die App-Welt unter iOS zu verbessern. Zwar führt Apple eine Kontrolle aller eingereichten Apps durch, diese ist aber nicht nur lückenhaft, sondern greift auch bei Sicherheitslücken nicht. Schließlich befindet sich Whatsapp als Negativbeispiel noch immer im App Store, obwohl die Anwendung mehrfach durch Sicherheitsprobleme aufgefallen ist. Derartiges Testen von Apps ist aufwendig, und dementsprechend werden nur wenige Apps überhaupt umfassend untersucht. Außerdem dürften zahlreiche Entwickler entdeckt werden, die allzu viele Daten sammeln.

Snoop-It beherrscht auch Verschleierungstaktiken. So kann die Anwendung auch Apps untersuchen, die das System nach verräterischen Hinweisen auf einen Jailbreak überprüfen und somit nicht starten würden. Snoop-It verbirgt einige dieser Hinweise, wie etwa Symlinks, Cydia oder manipulierte Dateirechte, die durch das Jailbreaken entstanden sind.

Die App Snoop-It soll noch vor Ende des Jahres erscheinen. Sie wird voraussichtlich über den Cydia-Store und Github verteilt. Der Quellcode wird laut Kurtz erst im nächsten Jahr bereitgestellt. Snoop-It setzt ein iOS-Gerät voraus und der Anwender muss in der Lage sein, einen Jailbreak durchzuführen. Ein paar Grundkenntnisse sind also notwendig. Eine Umsetzung auf Android ist derzeit nicht geplant.

SNOOP-IT FÜR IOS

Sicherheitschecks von iPhone-Apps für fast jeden möglich

Deepsec 2012 Die Snoop-It-App soll jedem eine Basisüberprüfung der Sicherheit von Apps ermöglichen. Das könnte dazu führen, dass viele iOS-Entwickler entdeckt werden, die auf fragwürdige Art und Weise Daten erheben.

Andreas Kurtz von den NESO Security Labs und der Universität Erlangen-Nürnberg arbeitet an einem einfach zu bedienenden Werkzeug, um iOS-Anwendungen auf ihre Sicherheit hin zu überprüfen. Die Snoop-It-App wird auf einem iPhone oder iPad installiert und dort über einen simplen Dialog konfiguriert. Kurtz demonstrierte die Anwendung, die sich noch in einem Vorversionsstatus befindet, auf der Deepsec in Wien. Dabei fiel auf, dass sie vergleichsweise einfach zu bedienen ist. Das Herumhacken auf der Kommandozeile ist nicht einmal notwendig. Stattdessen nutzt der Anwender einfach einen Browser und verbindet sich mit der Snoop-It-App, die gerade eine App untersucht.

1 / 5

Snoop-It-Demo

Snoop-It kann auch Anwendungen untersuchen, die bei einem Jailbreak nicht mehr starten. (Bild: Andreas Sebayang/Golem.de)

Datum: 29.11.2012, 15:08

Autor: Andreas Sebayang

Themen: Deepsec, App, Cydia, Passwort, Sicherheitslücke, iOS, Server, Security, Softwareentwicklung

Teilen: 0 27 30 12

Tools: Drucken

Über den Browser kann dann mit den Sicherheitstests begonnen werden. Einige dieser Tests sind sehr einfach gehalten. So ist es etwa möglich, der App einen anderen Ort vorzugaukeln. Die Auswahl geschieht über Google Maps. Interessant ist das, um etwa eine Kontrolle von Apps zu ermöglichen, die nur in bestimmten Arealen, etwa dem Firmengelände, benutzt werden dürfen. Auch der Netzwerkverkehr kann untersucht werden. So sieht der Anwender, ob und wie die App auf externe Server zugreift und erhobene Daten abliefert und ob dies verschlüsselt geschieht. Zugriffe auf Systemkomponenten (Schlüsselbund, Dateien, Kontakte und Fotos) werden ebenfalls aufgenommen.

Mit Hilfe eines Ampelsystems werden kritische Zugriffe außerdem schnell erfassbar gemacht. Zudem kann der Anwender Hardware-IDs (MACs und UDID) fälschen, um zu sehen, wie die App darauf reagiert. Bekanntlich nutzen einige Apps, darunter auch das populäre Whatsapp, diese als feste Passwörter.

Potenzial für eine umfassende Sicherheitsüberprüfung des App-Katalogs

Die Snoop-It-App hat das Potenzial, die App-Welt unter iOS zu verbessern. Zwar führt Apple eine Kontrolle aller eingereichten Apps durch, diese ist aber nicht nur lückenhaft, sondern greift auch bei Sicherheitslücken nicht. Schließlich befindet sich Whatsapp als Negativbeispiel noch immer im App Store, obwohl die Anwendung mehrfach durch Sicherheitsprobleme aufgefallen ist. Derartiges Testen von Apps ist aufwendig, und dementsprechend werden nur wenige Apps überhaupt umfassend untersucht. Außerdem dürften zahlreiche Entwickler entdeckt werden, die allzu viele Daten sammeln.

Snoop-It beherrscht auch Verschleierungstaktiken. So kann die Anwendung auch Apps untersuchen, die das System nach verräterischen Hinweisen auf einen Jailbreak überprüfen und somit nicht starten würden. Snoop-It verbirgt einige dieser Hinweise, wie etwa Symlinks, Cydia oder manipulierte Dateirechte, die durch das Jailbreaken entstanden sind.

Die App Snoop-It soll noch vor Ende des Jahres erscheinen. Sie wird voraussichtlich über den Cydia-Store und Github verteilt. Der Quellcode wird laut Kurtz erst im nächsten Jahr bereitgestellt. Snoop-It setzt ein iOS-Gerät voraus und der Anwender muss in der Lage sein, einen Jailbreak durchzuführen. Ein paar Grundkenntnisse sind also notwendig. Eine Umsetzung auf Android ist derzeit nicht geplant. ▪

https://adainitiative.org/2012/10/conferences-are-not-intended-to-create-bad-memories-only-good-ones-deepsec-organizer-ren-pfeiffer/

“Conferences are not intended to create bad memories, only good ones”

DeepSec organizer René Pfeiffer

Datum: 01.10.2012

Autor: Valerie Aurora

DeepSec logoDeepSec is the second hacker conference to adopt a public, enforceable anti-harassment policy in response to the Ada Initiative’s article about pervasive harassment of women at several hacker conferences (which called out DeepSec’s existing reputation as one of the most welcoming conferences for women).

We interviewed René Pfeiffer, one of the organizers of DeepSec about the conference, why they adopted a policy, and what they are looking forward to at future DeepSec conferences. It sounds like a great conference from all reports!

Tell us a little about DeepSec.

DeepSec’s full name is “In-Depth Security Conference”. The focus is on information security, and we like to present content which is not purely driven by marketing purposes. We are not a simple tradeshow with a “IT security” sticker slapped on the schedule. We try to be a platform where members of the academic community, governments, industry and (underground) hacking community meet in order to talk about security and exchange ideas. We believe in keeping an open mind and tearing down artificial barriers between groups that have a lot to talk about, but can’t in their normal environment. Most security related problems get worse if communication breaks down, so talking to each other is an important aspect of dealing with security breaches. This is what CERTs are preaching and what DeepSec tries to implement on conference-level.

The advantage to meet in person and talk and discuss certain issues from each perspective will give everyone involved a brighter understanding about needs and topics in the vast field of IT security, combined by interesting talks and new business opportunities.

The DeepSec event itself consists of two days of trainings followed by a two-day conference. We organise a dinner for all speakers and staff, and we have a party at the Metalab, a local hacker space, after the conference.

How did DeepSec get started?

In 2007 Paul Böhm created the DeepSec conference from scratch because he felt that a security-related conference where everyone can attend and talk openly was missing. He selected Vienna, Austria, as location which has been traditionally a bridge between different regions. Paul put a lot of effort into the first DeepSec and did a terrific job to kick-start it into existence.

What made you decide to adopt an anti-harassment policy?

There were two motivations. The first one were the experiences from other events participants wrote about. While we don't feel that conferences and events turn into places of harassment in general, we like to do our part to work against this. It really doesn't matter if there was a case already or not. The second motivation stems from the place DeepSec wants to be. We have a very international audience with roots in four different continents. If we want to create an atmosphere where everyone feels relaxed and is treated with respect, then we have to actively maintain this environment. Trust, respect and safe places do not automatically exist, they have to be created; you need people who care and who make sure an event stays hospitable.

Fortunately our staff cares, so our anti-harassment policy is really a statement of what we have been doing and trying to create since the first conference anyway.

What would you like to see at the next DeepSec?

We would like to see more people holding presentations and workshops who are not sure if their skills are "in-depth" enough, or who are not sure if they can handle speaking on stage. We actively support students with bright ideas with our under 21 category, and we will maintain a mixture of seasoned security experts and those who like a chance to become one. Everyone needs a start. Fresh perspectives never hurt, and we will actively support you if you let us know about the work you have done or are doing.

And for all the companies that are listening, please do not always think in leads when dealing with IT security. Be part of the community instead and show this proudly. Companies can have open minds, too.

Anything else you'd like to say?

We are well aware that small conferences have a lot of advantages compared to big events when it comes to publishing and enforcing an anti-harassment policy or protecting all attendees. If you are part of a team organising one of these big events, please consider to signal everyone thinking about attending that you want everyone to enjoy the talks, to have fun and not to be harassed for any reason. While you cannot control every single

situation and second of your event, you can clearly state what you expect from everyone being there, and you can

instruct your staff to do the same. It's a simple step. Conferences are not intended to create bad memories, only good ones.

The DeepSec and BruCON anti-harassment policies would not exist without the Ada Initiative's work. We are a non-profit funded primarily by donations from people like you. If you believe more women should attend hacker conferences, please become a supporting donor today.

Ada Initiative

Supporting women in open technology and culture

“Conferences are not intended to create bad memories, only good ones” DeepSec organizer René Pfeiffer

DeepSec is the second hacker conference to adopt a public, enforceable anti-harassment policy in response to the Ada Initiative’s article about pervasive harassment of women at several hacker conferences (which called out DeepSec’s existing reputation as one of the most welcoming conferences for women).

We interviewed René Pfeiffer, one of the organizers of DeepSec about the conference, why they adopted a policy, and what they are looking forward to at future DeepSec conferences. It sounds like a great conference from all reports!

Tell us a little about DeepSec.

DeepSec’s full name is “In-Depth Security Conference”. The focus is on information security, and we like to present content which is not purely driven by marketing purposes. **We are not a simple tradeshow with a “IT security” sticker slapped on the schedule.** We try to be a platform where members of the academic community, governments, industry and (underground) hacking community meet in order to talk about security and exchange ideas. We believe in keeping an open mind and tearing down artificial barriers between groups that have a lot to talk about, but can’t in their normal environment. Most security related problems get worse if communication breaks down, so talking to each other is an important aspect of dealing with security breaches. This is what CERTs are preaching and what DeepSec tries to implement on conference-level.

The advantage to meet in person and talk and discuss certain issues from each perspective will give everyone involved a brighter understanding about needs and topics in the vast field of IT security, combined by interesting talks and new business opportunities.

The DeepSec event itself consists of two days of trainings followed by a two-day conference. We organise a dinner for all speakers and staff, and we have a party at the Metalab, a local hacker space, after the conference.

How did DeepSec get started?

In 2007 Paul Böhm created the DeepSec conference from scratch because he felt that a security-related conference where everyone can attend and talk openly was missing. He selected Vienna, Austria, as location which has been traditionally a bridge between different regions. Paul put a lot of effort into the first DeepSec and did a terrific job to kick-start it into existence.

What made you decide to adopt an anti-harassment policy?

There were two motivations. The first one were the experiences from other events participants wrote about. While we don't feel that conferences and events turn into places of harassment in general, we like to do our part to work against this. It really doesn't matter if there was a case already or not. The second motivation stems from the place DeepSec wants to be. We have a very international audience with roots in four different continents. If we want to create an atmosphere where everyone feels relaxed and is treated with respect, then we have to actively maintain this environment. **Trust, respect and safe places do not automatically exist, they have to be created**; you need people who care and who make sure an event stays hospitable.

Fortunately our staff cares, so our anti-harassment policy is really a statement of what we have been doing and trying to create since the first conference anyway.

What would you like to see at the next DeepSec?

We would like to see more people holding presentations and workshops who are not sure if their skills are "in-depth" enough, or who are not sure if they can handle speaking on stage. We actively support students with bright ideas with our under 21 category, and we will maintain a mixture of seasoned security experts and those who like a chance to become one. Everyone needs a start. Fresh perspectives never hurt, and we will actively support you if you let us know about the work you have done or are doing.

And for all the companies that are listening, please do not always think in leads when dealing with IT security. Be part of the community instead and show this proudly. Companies can have open minds, too.

Anything else you'd like to say?

We are well aware that small conferences have a lot of advantages compared to big events when it comes to publishing and enforcing an anti-harassment policy or protecting all attendees. If you are part of a team organising one of these big events, please consider to signal everyone thinking about attending that you want everyone to enjoy the talks, to have fun and not to be harassed for any reason. While you cannot control every single situation and second of your event, you can clearly state what you expect from everyone being there, and

you can instruct your staff to do the same. It's a simple step. **Conferences are not intended to create bad memories, only good ones.**

The DeepSec and BruCON anti-harassment policies would not exist without the Ada Initiative's work. We are a non-profit funded primarily by donations from people like you. If you believe more women should attend hacker conferences, please become a supporting donor today.

This entry was posted in Ada Initiative resources in use, Anti-harassment policy, Interviews on October 1, 2012 [https://adainitiative.org/2012/10/conferences-are-not-intended-to-create-bad-memories-only-good-ones-deepsec-organizer-ren-pfeiffer/] by Valerie Aurora.

http://www.golem.de/news/paul-mockapetris-mit-dns-laesst-sich-noch-viel-machen-1208-94109.html

PAUL MOCKAPETRIS

“Mit DNS lässt sich noch viel machen”

Datum: 27.8.2012

Autor:Jörg Thoma

Das DNS-Protokoll ist noch nicht veraltet, könnte aber künftig durch neue Technik ersetzt werden, sagt dessen Erfinder Paul Mockapetris in einem Interview mit Golem.de. Und DNS sei der ideale Ort für Filter.

"Wer möchte schon auf einer Webseite mit Malware oder kinderpornografischem Material landen", fragt Paul Mockapetris zurück, als wir wissen wollen, ob er Filter per DNS immer noch befürworte. Und DNS habe noch viel Potenzial. Er könne sich beispielsweise dort eine integrierte Suche vorstellen, sagt er im Interview mit Golem.de.

Video: Paul Mockapetris über DNSSec, DNS Filtering und IPv6 (4:59)

Mockapetris geriet 2009 in die Kritik, als bekanntwurde, dass Nominum die Technik zur Filterung per DNS entwickeln würde, die in Deutschland geplant war, aber nach massiven Protesten wieder verworfen wurde.
Ganz nachvollziehen kann Mockapetris die Aufregung nicht: Die ISP sollten zwei Versionen von DNS anbieten, eine gefilterte, die gefährliche oder kriminelle Webseiten für diejenigen ausblendet, die gefahrlos surfen wollen, und eine für diejenigen, die aus Recherchegründen auch zweifelhafte Seiten ansteuern wollen.

DNSSec ist nicht genug

DNSSec eigne sich nur bedingt, die Sicherheitsprobleme im Internet zu lösen, denn es stelle nur sicher, dass Anfragen nicht gefälscht seien. Es gebe aber genügend Webseiten, die legitimiert von Kriminellen betrieben würden, sagt er.
Sir Tim Berners-Lee ist da anderer Meinung. DNS sei fast die einzige zentrale Instanz in einem sonst dezentralen Internet, sagte er in seiner Keynote-Ansprache auf der Campus Party Europe 2012. Berners-Lee setzte sich in seiner Rede für ein vollkommen freies, dezentrales und unzensiertes Internet ein. Er überlege, HTTP so zu erweitern, dass es bei Bedarf als Peer-to-Peer-Protokoll genutzt werden kann, auch um Zensur zu vermeiden.

DNS lässt sich noch erweitern

DNS habe aber noch sehr viel mehr Potenzial, als nur als Reputationsfilter eingesetzt zu werden, sagte Mockapetris. Es könne beispielsweise so erweitert werden, dass es als Suche verwendet werden könne.

In Kombination mit IPv6 stellt DNS aber kein Problem dar. DNS wurde so konzipiert, dass es bis zu 64.000 Datentypen nutzen kann, gegenwärtig werden aber nur etwa 60 genutzt. Es gebe andere Probleme mit dem neuen Internetprotokoll, etwa die gleichzeitige Nutzung von IPv4 und IPv6. Ähnlich äußerte sich auch der Netzwerkexperte Fernando Gont auf der Sicherheitskonferenz Deepsec im November 2011.

Er selbst wolle sich zukünftig der Weiterentwicklung von DNS im Zusammenhang mit Inhalten widmen, sagte Mockapetris. "Vielleicht ergibt sich daraus die nächste Generation von DNS."

PAUL MOCKAPETRIS

"Mit DNS lässt sich noch viel machen"

Das DNS-Protokoll ist noch nicht veraltet, könnte aber künftig durch neue Technik ersetzt werden, sagt dessen Erfinder Paul Mockapetris in einem Interview mit Golem.de. Und DNS sei der ideale Ort für Filter.

Paul Mockapetris sprach in einem Interview mit Golem.de über die Zukunft von DNS. (Bild: Daniel Pook/Golem.de)

Datum: 27.8.2012, 15:43

Autor: Jörg Thoma

Themen: DNS, Campus Party, IPv6, Malware, Server-Applikationen, Tim Berners-Lee, Zensur, Applikationen

Teilen: 0 7 15 22

Tools: Drucken

"Wer möchte schon auf einer Webseite mit Malware oder kinderpornografischem Material landen", fragt Paul Mockapetris zurück, als wir wissen wollen, ob er Filter per DNS immer noch befürworte. Und DNS habe noch viel Potenzial. Er könne sich beispielsweise dort eine integrierte Suche vorstellen, sagt er im Interview mit Golem.de.

Video: Paul Mockapetris über DNSSec, DNS Filtering und IPv6 (4:59)

Mockapetris geriet 2009 in die Kritik, als bekanntwurde, dass Nominum die Technik zur Filterung per DNS entwickeln würde, die in Deutschland geplant war, aber nach massiven Protesten wieder verworfen wurde.

Ganz nachvollziehen kann Mockapetris die Aufregung nicht: Die ISP sollten zwei Versionen von DNS anbieten, eine gefilterte, die gefährliche oder kriminelle Webseiten für diejenigen ausblendet, die gefahrlos surfen wollen, und eine für diejenigen, die aus Recherchegründen auch zweifelhafte Seiten ansteuern wollen.

DNSSec ist nicht genug

DNSSec eigne sich nur bedingt, die Sicherheitsprobleme im Internet zu lösen, denn es stelle nur sicher, dass Anfragen nicht gefälscht seien. Es gebe aber genügend Webseiten, die legitimiert von Kriminellen betrieben würden, sagt er.

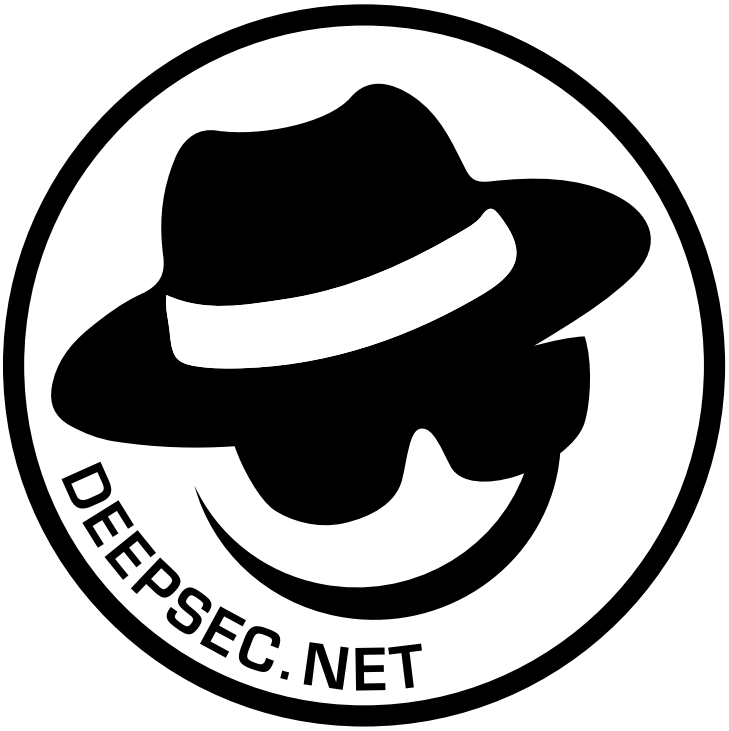
Sir Tim Berners-Lee ist da anderer Meinung. DNS sei fast die einzige zentrale Instanz in einem sonst dezentralen Internet, sagte er in seiner Keynote-Ansprache auf der Campus Party Europe 2012. Berners-Lee setzte sich in seiner Rede für ein vollkommen freies, dezentrales und unzensiertes Internet ein. Er überlege, HTTP so zu erweitern, dass es bei Bedarf als Peer-to-Peer-Protokoll genutzt werden kann, auch um Zensur zu vermeiden.

DNS lässt sich noch erweitern

DNS habe aber noch sehr viel mehr Potenzial, als nur als Reputationsfilter eingesetzt zu werden, sagte Mockapetris. Es könne beispielsweise so erweitert werden, dass es als Suche verwendet werden könne.

In Kombination mit IPv6 stellt DNS aber kein Problem dar. DNS wurde so konzipiert, dass es bis zu 64.000 Datentypen nutzen kann, gegenwärtig werden aber nur etwa 60 genutzt. Es gebe andere Probleme mit dem neuen Internetprotokoll, etwa die gleichzeitige Nutzung von IPv4 und IPv6. Ähnlich äußerte sich auch der Netzwerkexperte Fernando Gont auf der Sicherheitskonferenz Deepsec im November 2011.

Er selbst wolle sich zukünftig der Weiterentwicklung von DNS im Zusammenhang mit Inhalten widmen, sagte Mockapetris. *"Vielleicht ergibt sich daraus die nächste Generation von DNS."* ▪


DEEPSEC.NET

http://www.pressebox.de/inaktiv/deepsec-gmbh/Vorlaeufiges-DeepSec-Programm-veroeffentlicht-Cyberwar-und-Sicherheit-von-Mobilfunknetzwerken-im-Konferenz-Fokus/boxid/541775

Pressemitteilung BoxID 541775

Autor: René Pfeiffer

Datum.25.09.2012

Vorläufiges DeepSec-Programm veröffentlicht:
Cyberwar und Sicherheit von Mobilfunknetzwerken im Konferenz-Fokus
Internationale Security-Expertise in 33 Vorträgen und acht Workshops

(PresseBox) (Wien, 25.09.2012) Vom 27. bis zum 30. November trifft sich die internationale Elite der Network-Security- und Hacking-Branche zum sechsten Mal auf der Wiener Sicherheitskonferenz DeepSec (https://deepsec.net/). 2012 liegen die Konferenzschwerpunkte auf der Sicherheit von mobilen Geräten, M obilfunknetzwerken und dem Cyberwar. 33 Vorträge und acht Workshops informieren Anwender, Forscher, IT- und Security-Unternehmen, Behörden sowie die Hacker-Community über die relevanten Cyber-Sicherheitsthemen der Gegenwart. "Für die sechste DeepSec konnten wir mit Felix Lindner und Babak Javadi internationale Spitzen-Referenten gewinnen und somit die Besten auf ihrem Gebiet in Wien vereinen", erklärt René Pfeiffer, Organisator der DeepSec.

Traditionell werden die ersten beiden Konferenztage aus acht Workshops bestehen. Mit Harald Welte und Dieter Spaar (Independent Researcher & HMW-Consulting) wird die DeepSec die führenden Experten für Mobilfunksicherheit nach Wien bringen. Ihr Workshop "Attacks on GSM Networks" beschäftigt sich mit den Schwächen aktueller GSM-Sicherheitssoftware und verdeutlicht, welche Probleme Sicherheitskräfte mit derzeit verfügbaren Tools haben. Die zweite Hälfte des Workshops wird aus Praxis-Ausflügen in GSM-Sicherheitstools wie OsmocomBB, OpenBSC, airprobe und SIMtrace bestehen.

Der zweitägige DeepSec-Workshop "Social Engineering Training for IT Security Professionals" der britischen Sicherheitsexperten Sharon Conheady und Martin Law der Firma First Defence Information Security Ltd., kommt DeepSec-Kennern sicher bekannt vor. Tatsächlich verliert die Gefahr sogenannter Social-Engineering-Angriffe gerade für größere Unternehmen nichts ihrer Bedrohlichkeit. Perfide Social Engineers versuchen dabei gezielt unsichere Mitarbeiter am Telefon auszuspionieren. Oft versuchen sie es mit der Telefon-Masche. Als vermeintliche Vorgesetzte fordern sie von Mitarbeitern sofort wichtige Auskünfte. Gerade gegenüber vermeintlichen Vorgesetzten ist die natürliche menschliche Reaktion eine konfliktvermeidende und kooperative. In Trainings erfahren Interessenten, wie sie sich selbst und ihre Mitarbeiter vor solchen Attacken schützen können. Der Workshop wird aus einem theoretischen und einem praktischen Teil bestehen.

Der Onapsis-Mitarbeiter Juan Pablo Perez Etchegoyen widmet sich in seinem SAP-Security-Workshop "SAP Security In-Depth" der Absicherung von SAP-Systemen in großen Firmen. Der CTO von Onapsis beschäftigt sich auch in seinem Vortrag "Inception of the SAP Platform's Brain: Attacks to SAP Solution Manager" mit der SAP-Sicherheit. Diese Themen sind von besonderem Interesse für alle SAP-Anwender und -Entwickler.

Etchegoyens Beitrag ist einer der am 29. November startenden 33 Vorträge. Die Keynote wird in diesem Jahr vom Leiter der Recurity Labs, Felix "FX" Lindner gehalten. Lindners Vortrag "We came in Peace - They don't: Hackers vs. CyberWar" thematisiert das derzeit kursierende Cyberwar-Gespenst im Zusammenhang mit Sicherheitslücken in der digitalen Waffenhandel-Industrie. Auch die Referenten Stefan Schumacher (Magdeburger Institut für Sicherheitsforschung) und Karin Kosina widmen sich dem Thema Cyberwar. Schumacher spricht in "The Vienna Programme: A Global Strategy for Cyber Security by the Global Cyber Defence Initiative" über Initiativen, Cyberwar durch Kommunikation in Krisensituationen zu vermeiden. Kosina setzt die Thematik Cyberwar mit "Wargames in the Fifth Domain" in einen internationalen Kontext, der stark die völker- und kriegsrechtliche Seite betont und verbindet diese Felder mit den verfügbaren technischen Möglichkeiten.

Mit Babak Javadi ist auch der Gründer der CORE Group in Wien zu Gast. In seinem Vortrag "4140 Ways Your Alarm System Can Fail" beschäftigt er sich mit der generellen Anfälligkeit herkömmlicher Alarmanlagen. Michael Niekamp und Florian Grunert von der Universität Osnabrück ergänzen das Thema mit ihrem Vortrag "A Non-Attribution-Dilemma and it's Impact on Legal Regulation of Cyberwar" durch eine rein rechtliche Situationsbetrachtung. Am 30. November kommt mit Robert M. Lee noch ein Angehöriger der US Air Force zu Wort: Sein Vortrag "The Interim Years of Cyberspace - Security in a Domain of Warfare" wirft einen Blick auf die Geschichte des Cyberwar. "Gerade den Cyberwar kennen selbst viele Computer-affine Menschen nur aus Kinofilmen oder Tom-Clancy-Videospielen. Wir wollen mit den Vorträgen auf der DeepSec 2012 einen Bezug zur Realität herstellen und das Thema sachlich diskutieren. Gerade beim Thema Infrastruktur und Sicherheit kommt es auf Fakten und Details an", erklärt Pfeiffer.

Die DeepSec versteht sich aber nicht nur als Expertenforum, sondern will gezielt Vorurteile gegenüber ihrer Zielgruppe abbauen. Weder seien DeepSec-Besucher kriminelle Hacker, noch Weltuntergangs-Nerds, so Pfeiffer. Zudem laden die DeepSec-Referenten ausdrücklich zum direkten Dialog ein. Während der ganzen DeepSec Konferenz werden die Besucher Zeit für persönliche Gespräche mit den Experten haben.
Weitere Informationen und das Programm der DeepSec finden Sie hier: https://deepsec.net/
Anmeldung zur DeepSec unter: https://deepsec.net/register.html

Vorläufiges DeepSec-Programm veröffentlicht: Cyberwar und Sicherheit von Mobilfunknetzwerken im Konferenz-Fokus

Internationale Security-Expertise in 33 Vorträgen und acht Workshops

(PresseBox) (Wien, 25.09.2012) Vom 27. bis zum 30. November trifft sich die internationale Elite der Network-Security- und Hacking-Branche zum sechsten Mal auf der Wiener Sicherheitskonferenz DeepSec (https://deepsec.net/). 2012 liegen die Konferenzschwerpunkte auf der Sicherheit von mobilen Geräten, M obilfunknetzwerken und dem Cyberwar. 33 Vorträge und acht Workshops informieren Anwender, Forscher, IT- und Security-Unternehmen, Behörden sowie die Hacker-Community über die relevanten Cyber-Sicherheitsthemen der Gegenwart. "Für die sechste DeepSec konnten wir mit Felix Lindner und Babak Javadi internationale Spitzen-Referenten gewinnen und somit die Besten auf ihrem Gebiet in Wien vereinen", erklärt René Pfeiffer, Organisator der DeepSec.

Traditionell werden die ersten beiden Konferenztage aus acht Workshops bestehen. Mit Harald Welte und Dieter Spaar (Independent Researcher & HMW-Consulting) wird die DeepSec die führenden Experten für Mobilfunksicherheit nach Wien bringen. Ihr Workshop "Attacks on GSM Networks" beschäftigt sich mit den Schwächen aktueller GSM-Sicherheitssoftware und verdeutlicht, welche Probleme Sicherheitskräfte mit derzeit verfügbaren Tools haben. Die zweite Hälfte des Workshops wird aus Praxis-Ausflügen in GSM-Sicherheitstools wie OsmocomBB, OpenBSC, airprobe und SIMtrace bestehen.

Der zweitägige DeepSec-Workshop "Social Engineering Training for IT Security Professionals" der britischen Sicherheitsexperten Sharon Conheady und Martin Law der Firma First Defence Information Security Ltd., kommt DeepSec-Kennern sicher bekannt vor. Tatsächlich verliert die Gefahr sogenannter Social-Engineering-Angriffe gerade für größere Unternehmen nichts ihrer Bedrohlichkeit. Perfide Social Engineers versuchen dabei gezielt unsichere Mitarbeiter am Telefon auszuspionieren. Oft versuchen sie es mit der Telefon-Masche. Als vermeintliche Vorgesetzte fordern sie von Mitarbeitern sofort wichtige Auskünfte. Gerade gegenüber vermeintlichen Vorgesetzten ist die natürliche menschliche Reaktion eine konfliktvermeidende und kooperative. In Trainings erfahren Interessenten, wie sie sich selbst und ihre Mitarbeiter vor solchen Attacken schützen können. Der Workshop wird aus einem theoretischen und einem praktischen Teil bestehen.

Der Onapsis-Mitarbeiter Juan Pablo Perez Etchegoyen widmet sich in seinem SAP-Security-Workshop "SAP Security In-Depth" der Absicherung von SAP-Systemen in großen Firmen. Der CTO von Onapsis beschäftigt sich auch in seinem Vortrag "Inception of the SAP Platform's Brain: Attacks to SAP Solution Manager" mit der SAP-Sicherheit. Diese Themen sind von besonderem Interesse für alle SAP-Anwender und -Entwickler.

Etchegoyens Beitrag ist einer der am 29. November startenden 33 Vorträge. Die Keynote wird in diesem Jahr vom Leiter der Recurity Labs, Felix "FX" Lindner gehalten. Lindners Vortrag "We came in Peace - They don't: Hackers vs. CyberWar" thematisiert das derzeit kursierende Cyberwar-Gespenst im Zusammenhang mit Sicherheitslücken in der digitalen Waffenhandel-Industrie. Auch die Referenten Stefan Schumacher (Magdeburger Institut für Sicherheitsforschung) und Karin Kosina widmen sich dem Thema Cyberwar. Schumacher spricht in "The Vienna Programme: A Global Strategy for Cyber Security by the Global Cyber Defence Initiative" über Initiativen, Cyberwar durch Kommunikation in Krisensituationen zu vermeiden. Kosina setzt die Thematik Cyberwar mit "Wargames in the Fifth Domain" in einen internationalen Kontext, der stark die völker- und kriegsrechtliche Seite betont und verbindet diese Felder mit den verfügbaren technischen Möglichkeiten.

Mit Babak Javadi ist auch der Gründer der CORE Group in Wien zu Gast. In seinem Vortrag "4140 Ways Your Alarm System Can Fail" beschäftigt er sich mit der generellen Anfälligkeit herkömmlicher Alarmanlagen. Michael Niekamp und Florian Grunert von der Universität Osnabrück ergänzen das Thema mit ihrem Vortrag "A Non-Attribution-Dilemma and it's Impact on Legal Regulation of Cyberwar" durch eine rein rechtliche Situationsbetrachtung. Am 30. November kommt mit Robert M. Lee noch ein Angehöriger der US Air Force zu Wort: Sein Vortrag "The Interim Years of Cyberspace - Security in a Domain of Warfare" wirft einen Blick auf die Geschichte des Cyberwar. "Gerade den Cyberwar kennen selbst viele Computer-affine Menschen nur aus Kinofilmen oder Tom-Clancy-Videospielen. Wir wollen mit den Vorträgen auf der DeepSec 2012 einen Bezug zur Realität herstellen und das Thema sachlich diskutieren. Gerade beim Thema Infrastruktur und Sicherheit kommt es auf Fakten und Details an", erklärt Pfeiffer.

Die DeepSec versteht sich aber nicht nur als Expertenforum, sondern will gezielt Vorurteile gegenüber ihrer Zielgruppe abbauen. Weder seien DeepSec-Besucher kriminelle Hacker, noch Weltuntergangs-Nerds, so Pfeiffer. Zudem laden die DeepSec-Referenten ausdrücklich zum direkten Dialog ein. Während der ganzen DeepSec Konferenz werden die Besucher Zeit für persönliche Gespräche mit den Experten haben.

Weitere Informationen und das Programm der DeepSec finden Sie hier: https://deepsec.net/

Anmeldung zur DeepSec unter: https://deepsec.net/register.html

3. DACH-Sicherheitsforum Österreich

Kontakt

DeepSec GmbH
Weyringergasse 30a/10
A-1040 Wien

http://www.pressetext.com/news/20120523006

Datenrettung: "Bei Daten-Gau sind alle Security-Regeln plötzlich außer Kraft"
Attingo und DeepSec warnen: Datenrettungspartner sollten vorab auditiert werden

Datum: 23.05.2012

Autor: René Pfeiffer

Attingo Datenrettung - Labor

[Fotos]

Wien,Hamburg (pts006/23.05.2012/07:35) - Größere Unternehmen verfügen über ausgefeilte Security-Policies und Prozessbeschreibungen vom Backup bis zur Datenwiederherstellung. Was aber häufig unter den Tisch fällt, sind Notfallpläne für den Fall der Fälle: nämlich, wenn sich defekte Datenträger nicht hausintern wiederherstellen lassen und der Gang zum Datenretter erforderlich wird. "Bei kritischen Systemausfällen werden oft plötzlich zentrale Security-Regeln außer Acht gelassen und in Windeseile Server, RAID-Systeme oder Festplatten mit hochsensiblen Informationen an externe Dienstleister übergeben - ohne dass diese im Vorfeld auf Sicherheit geprüft wurden", berichtet René Pfeiffer, Geschäftsführer der Wiener Sicherheitskonferenz DeepSec.

Datendiebe zapfen Dritte an

Die Gefahr dabei: Einige Datenrettungsanbieter schicken defekte Medien an Recovery-Labore im benachbarten Ausland, ohne ihre Kunden explizit davon zu informieren. "Organisierte Datendiebe zapfen aber nicht selten Quellen über Dritte in Insider-Branchen an. Wenn auf diesem Weg Daten verloren gehen oder entwendet werden, hat das Unternehmen den doppelten Schaden", warnt Pfeiffer. Denn es kommt auch noch das Haftungsrisiko hinzu. "Laut Datenschutzgesetz haftet der Eigentümer dann voll für seine Informationen, wenn er es verabsäumt, die 'sichere Datenverarbeitung' durch seinen Dienstleister vorab zu prüfen", erklärt Nicolas Ehrschwendner, Geschäftsführer des heimischen Datenrettungsunternehmens Attingo. De facto fordert das DSG damit die Durchführung von Dienstleister-Audits.

Notfallplan für Datenrettung

Nach dem Motto: "Prüfe deinen Datenretter, so lange die IT-Welt noch in Ordnung ist", bietet Attingo seinen Kunden die gemeinsame Erarbeitung von Notfallplänen schon im Vorfeld an. Der Recovery-Spezialist betreibt sein Reinraumlabor in Wien, so dass ein Versand ins Ausland kein Thema ist. Aber mit seiner Strategie begegnet Attingo einer weiteren Gefahrenquelle: Bei Ausfall von Datenträgern liegt das größte technische Risiko in unsachgemäßen Wiederherstellungsversuchen. "In mehr als 80 Prozent aller Fälle, bei denen selbstständig Rettungsversuche unternommen werden, vergrößert sich der Schaden dadurch letztendlich", berichtet Ehrschwendner aus der täglichen

Praxis.

Typische Fehler

"Bei Ausfall von Servern oder RAID-Systemen werden in der Hektik oft hausintern Schritte unternommen, die zwar logisch erscheinen, aber aufgrund der Komplexität gerade diesmal nicht funktionieren", führt er aus. Typische Fehler sind etwa: unkontrolliertes Tauschen defekter Festplatten, Löschen und neu-Anlegen von RAID-Konfigurationen, das Erzwingen des Online-Status von RAIDs oder Ausprobieren von unbekannten Funktionen. Generell sind die Daten auf einem defekten Speichermedium im Reinraumlabor bis zu 100 Prozent rekonstruierbar, solange die betreffenden Sektoren nicht durch falsch veranlasste Vorgänge im Betriebssystem überschrieben wurden. Ein schädigender Vorgang kann aber schon ein simpler Systemstart sein.

Recovery-Partner in die Policy

Vor allem Banken, Health-Care- und Forschungsunternehmen mit sensiblen Daten nutzen verstärkt die Möglichkeit, gemeinsam mit den Recovery-Spezialisten von Attingo eigene Notfallpläne für die Datenrettung auszuarbeiten. Ein wesentlicher Punkt dabei ist, dass der Datenrettungspartner schon auditiert wird, lange bevor eine Katastrophe eintritt. Auch DeepSec Geschäftsführer René Pfeiffer empfiehlt: "Die Auswahl des Datenrettungspartners gehört konsequenterweise in die Security-Policy integriert."

Über DeepSec

Die DeepSec bringt als neutrale Plattform Sicherheitsexperten aus allen Bereichen zum Gedanken- und Erfahrungsaustausch zusammen. Die Konferenz will aber auch dem verbreiteten Vorurteil entgegenwirken, dass Hacker zwangsläufig Kriminelle sind. "Ganz im Gegenteil. Vielen sogenannten Hackern geht es eher darum, Sicherheitslücken aufzuzeigen und bekannt zu machen. Man kann nur Gefahren beseitigen, die man kennt und die erforscht sind, ganz so wie in anderen Bereichen", so Pfeiffer.

Weitere Informationen zur DeepSec finden Sie hier: https://deepsec.net/

Über Attingo Datenrettung

Attingo Datenrettung ist ein führender, europäischer Anbieter von Datenrettungen. Die Datenrettung befasst sich mit der Rekonstruktion von Daten, die durch Löschung, Formatierung, technische Defekte, Manipulation, Sabotage oder äußere Einflüsse wie Wasser oder Feuer beeinträchtigt wurden. Attingo rettet diese Daten. Das Unternehmen betreibt dazu modernste Reinraumlaboratorien in Wien, Hamburg und Amsterdam und verfügt über Experten mit jahrelanger Erfahrung. Attingo ist in Notfällen für seine Klienten 24/7 erreichbar.

Weitere Informationen: http://www.attingo.com/

Rückfragehinweis: DI Nicolas Ehrschwendner: +43(1)2360101, +49(40)5488756-0, presse@attingo.com

Aussender: Attingo Datenrettung GmbH

Die DeepSec bringt als neutrale Plattform Sicherheitsexperten aus allen Bereichen zum Gedanken- und Erfahrungsaustausch zusammen. Die Konferenz will aber auch dem verbreiteten Vorurteil entgegenwirken, dass Hacker zwangsläufig Kriminelle sind. "Ganz im Gegenteil. Vielen sogenannten Hackern geht es eher darum, Sicherheitslücken aufzuzeigen und bekannt zu machen. Man kann nur Gefahren beseitigen, die man kennt und die erforscht sind, ganz so wie in anderen Bereichen", so Pfeiffer.
Weitere Informationen zur DeepSec finden Sie hier: https://deepsec.net/

Über Attingo Datenrettung
Attingo Datenrettung ist ein führender, europäischer Anbieter von Datenrettungen. Die Datenrettung befasst sich mit der Rekonstruktion von Daten, die durch Löschung, Formatierung, technische Defekte, Manipulation, Sabotage oder äußere Einflüsse wie Wasser oder Feuer beeinträchtigt wurden. Attingo rettet diese Daten. Das Unternehmen betreibt dazu modernste Reinraumlaboratorien in Wien, Hamburg und Amsterdam und verfügt über Experten mit jahrelanger Erfahrung. Attingo ist in Notfällen für seine Klienten 24/7 erreichbar.
Weitere Informationen: http://www.attingo.com/

Rückfragehinweis: DI Nicolas Ehrschwendner: +43(1)2360101, +49(40)5488756-0, presse@attingo.com
Aussender: Attingo Datenrettung GmbH

(Ende)

Aussender:	Attingo Datenrettung GmbH
Ansprechpartner:	Dipl. Ing. Nicolas Ehrschwendner
Tel.:	+43 / 1 / 236 01 01
E-Mail:	ne@attingo.com
Website:	www.attingo.com

Contact

René Pfeiffer

rpfeiffer@deepsec.net

+43/676/5626390

DeepSec GmbH

c/o Mr. René Pfeiffer

Bräuhausgasse 32

1050 Vienna, Austria

VAT ID: ATU63522646

Business registration number: FN 294621 t

Customs EORI code: ATEOS1000025635