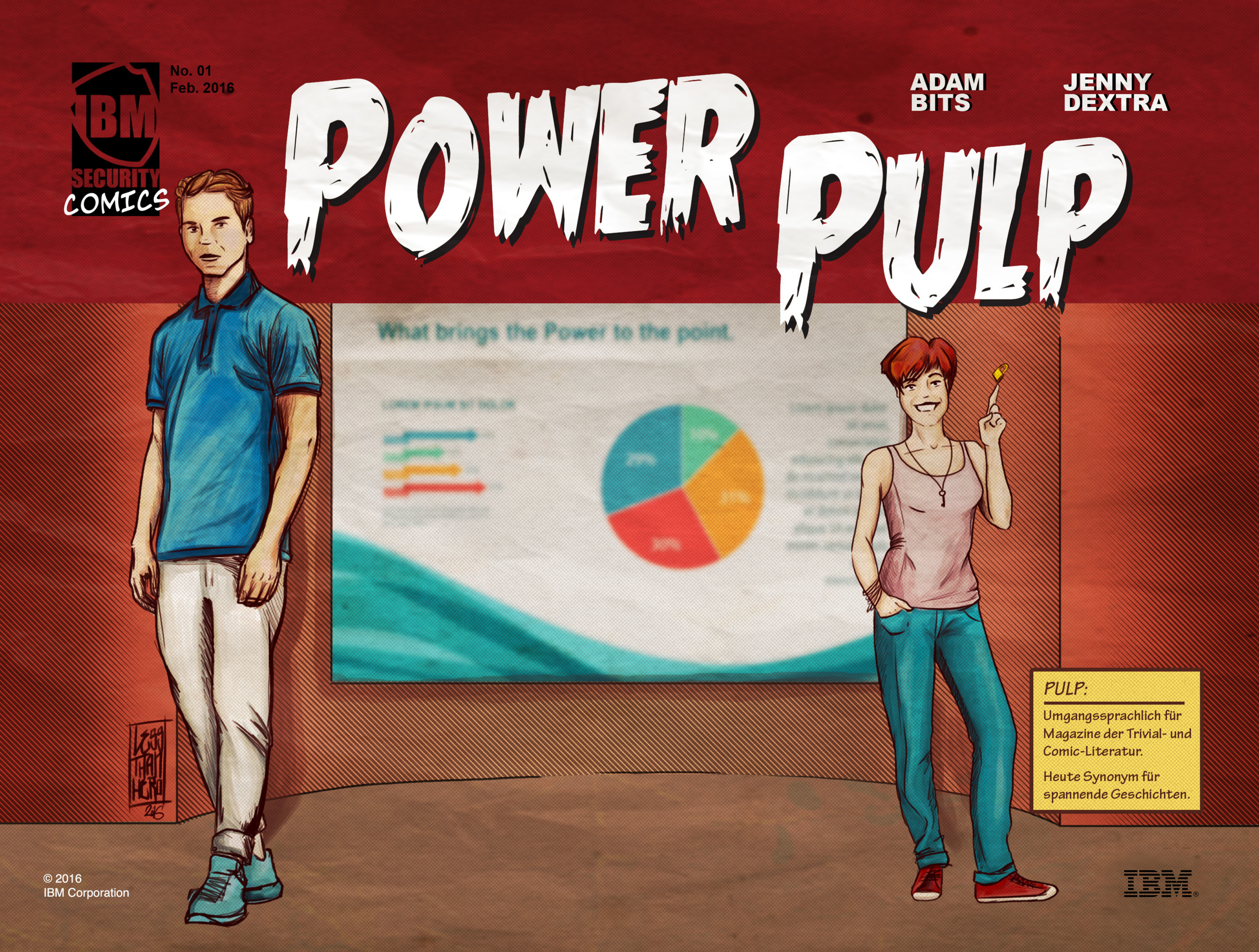
BM SECURITY COMICS
No. 01
Feb. 2016

POWER PULP

ADAM BITS
JENNY DEXTRA



PULP:

Umgangssprachlich für Magazine der Trivial- und Comic-Literatur.

Heute Synonym für spannende Geschichten.

IBM

„Wenn man bei ner Firma über IT-Sicherheit redet, heißt das meistens Powerpoint. Chart reiht sich an Chart. Protokolle. Filter. Zugangssicherheit.“

„Aber das real life hält sich nicht an Präsentationen. Man hat die üblichen Vorstellungen. Cooler Hacker. Business-orientierter CISO. Hoodie gegen Schlips. In Wahrheit sind sich beide Seiten dieses Kampfes viel ähnlicher, als man denkt.“

„Hacker sind oft in erster Linie eines: Geschäftsorientierte Service-Freelancer. Und CISOs sind so etwas wie Türsteher mit Budget. Kein Stoff für Powerpoint. “

„Mehr ne Geschichte.“

„Aber sehen Sie selbst ….“

„Nehmen wir Adam als Beispiel. Obwohl erst 34 Jahre alt, sieht er wenig Tageslicht. “

„Ex-Gamer. “

„Ex-Pizzabote.“

„Laufendes BWL-Studium.
Und wie er sich das finanziert…“

„…das wissen nur Wenige. Sagen wir so: Er makelt. Und zwar Informationen, deren Schutz ihren Besitzern nicht so viel wert ist, wie anderen der Zugang.“

„Früher war das mal ein Spiel. Heute wird so etwas hochprofessionell vermittelt. Über Talentbörsen. In Echtzeit. Skill-basiert. Anonym. “

„Tor sein Dank. Adam nennt das liebevoll sein „Hacker Harz“

„An diesem Montag fällt Adam ein besonderes Job-Bonbon in die Hände…“

„Der Auftrag lautet, vom Unternehmen MFG Health Patientenakten auszuleihen.“

„ - ohne Erlaubnis, versteht sich.“

„Krankenakten sind das Wertvollste, was man im Moment im Netz klauen kann“, denkt Adam. „Die Bluechips unter den sensiblen Daten. “

„Weit besser als ein gehackter Account. Und ungefähr 40 Mal so wertvoll.“
Er nimmt den Job an.“

„Google ist dein Freund“, denkt Adam, als er sich mit grundlegenden Informationen über MFG eindeckt.

„Die Zeit drängt allerdings. Aber Adam ist nicht nur von der schnellen, sondern auch von der gründlichen Truppe. Zeit für etwas eigene Grundlagenforschung …“

„Zum Glück gibt`s Skripte für die generische Schwachstellen-Analyse von Netzwerken. Mal sehen, was die Sicherheitsleute von MFG so drauf haben.“

IBM

IP Netzwerke funktionieren wie ein komplexes System kommunizierender Röhren.

Darin huschen die fleißigen Pakete hin und her. Eine prima Spielwiese für Attacken.

Das funktioniert so sicher wie ein Hütchenspiel.

Angestellte melden sich an.

Gehen auf die Seite.

Habe jetzt einige Hintertüren in Healthcare Firmen. Bloß bei MFG beißt sich der nagelneue Exploit wieder die Zähne aus.

Happy ZERO Day

Wenn Scripte die Arbeit machen, hat der Hacker mal kurz Pause.

Blöd nur, wenn das Script nix findet. Kann doch nicht sein. Keine vergessenen Patches? Keine offenen Ports?

Kein Ansatzpunkt für einen schönen „Man-in-the-Middle“ Code?

Jetzt packt mich der Ehrgeiz. Les mich ein bisschen in die Branche ein. Bastele einen Honeypot. Locke Leute aus diversen Healthcare Firmen an, damit sie einen interessanten Newsletter abonnieren. Gratis natürlich. Mit einem nagelneuen Cross Site Scripting Zero Exploit als Zugabe.

Register Here:

******

Wohlbefinden

HEALTH + CARE

SEND

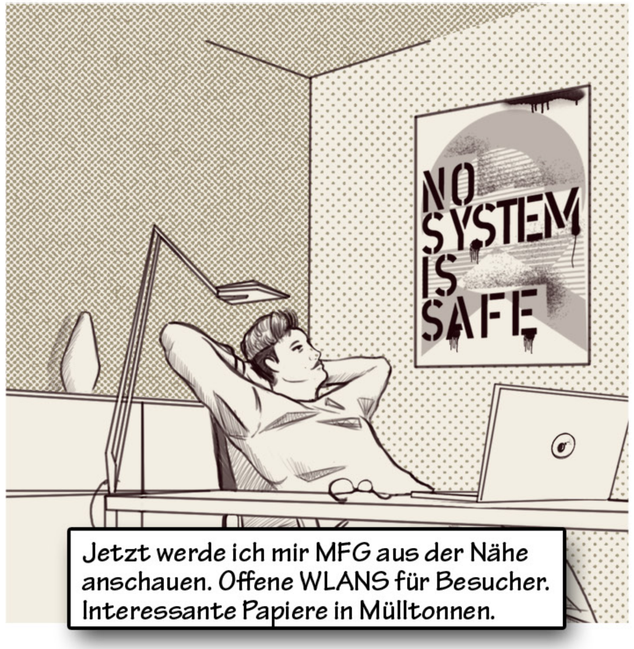
Ich schreibe meinem anonymen Auftraggeber: „Müssen es unbedingt MFG Patientendaten sein? Hätte welche von anderen Firmen im Angebot. Wie wäre es mit Firma X? Firma Y interessant?“

Die Antwort lässt keine Fragen offen. MFG Patientendaten oder keine. Mein Auftraggeber ist etwas unentspannt.

Vielleicht ist es sogar selber eine Healthcare Firma. Vielleicht sogar Firma x, deren Daten ich ihnen ersatzweise angeboten habe. Könnte glatt sein, so wie man mir antwortet.

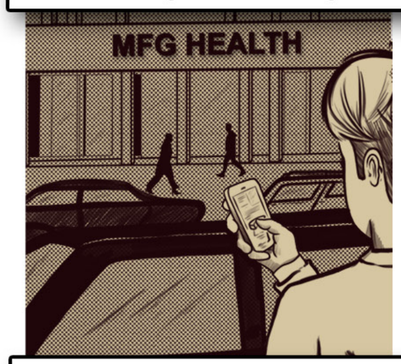
Was ich nicht weiß: Ich habe längst eine Gegenspielerin. Sie kennt mich nicht mal. Weiß nicht, was ich gerade versuche.

Benutzt aber anscheinend Sicherheitssysteme, die selbst allerneuesten Exploits standhalten. Als ob diese Systeme heuristisch Bedrohungen vorhersehen könnten.

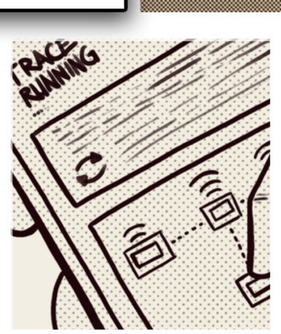


Jetzt werde ich mir MFG aus der Nähe anschauen. Offene WLANS für Besucher. Interessante Papiere in Mülltonnen.

Eine Bahnfahrt später stehe ich vor dem Gebäude. Gar nicht mal so protzig. Dezent. Keine große Firma. Und schlechtes Wetter. Liebt man, wenn man unauffällig sein will. Die Menschen sind ganz mit sich und ihren Wegen beschäftigt.

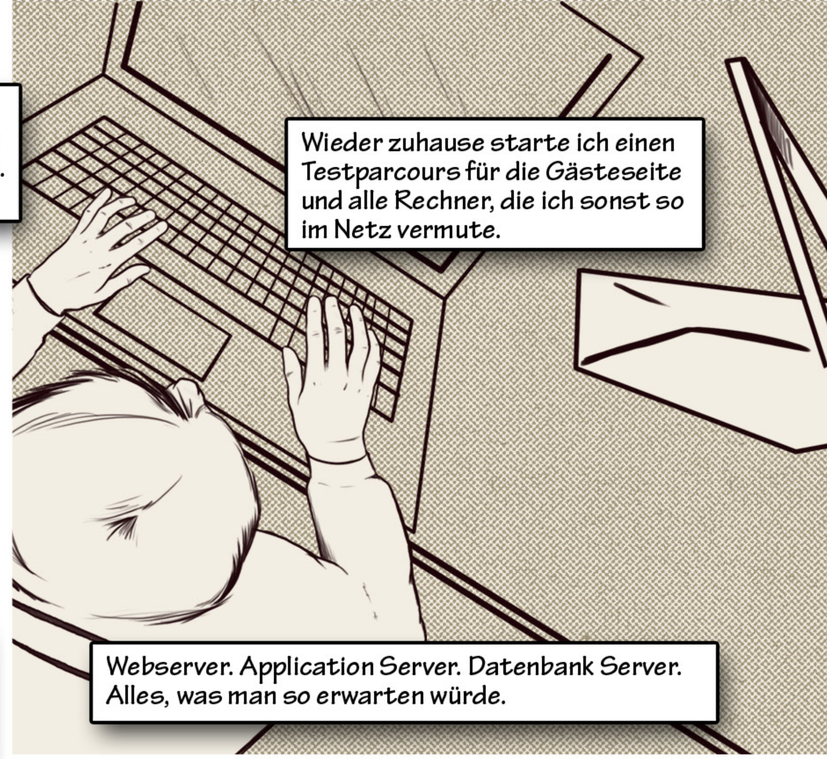


Ich steh da so rum und mach ein bisschen auf WLAN Client. Kriege aber bloß einen Gäste-WLAN rein, der über eine Website-Anmeldung gesichert ist.



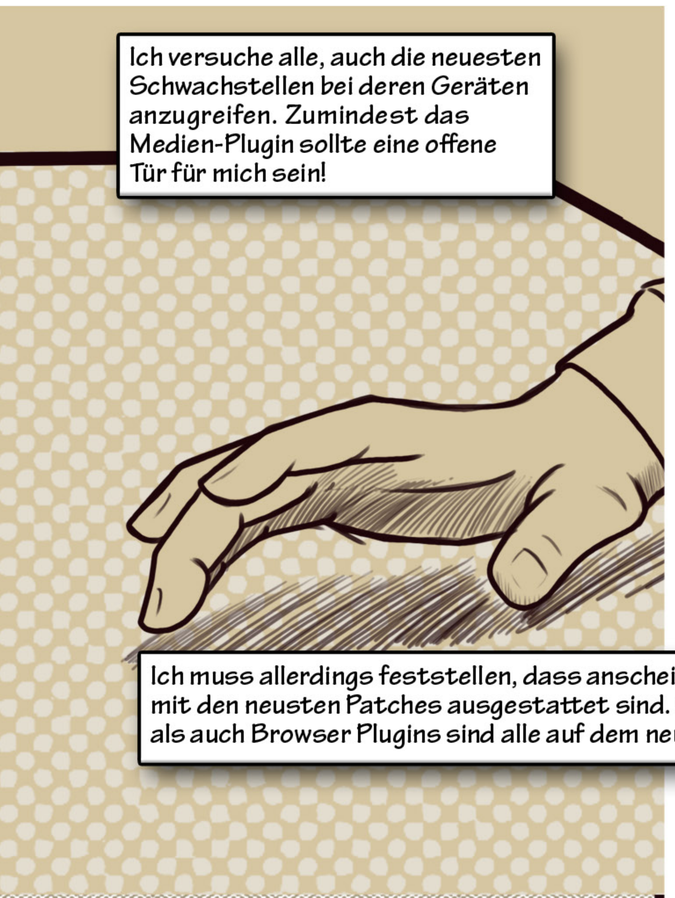
So ohne weiteres komm ich nicht rein. Allerdings ist auf der Gäste-Anmelde-Seite ein internes Business TV Video eingeblendet. Werbung eben.

Das interne Video basiert auf einem Browser-Medien-Plugin, dass dafür bekannt ist, mehr Löcher zu haben, als ein Nudelsieb.



Wieder zuhause starte ich einen Testparcours für die Gästeseite und alle Rechner, die ich sonst so im Netz vermute.

Webserver. Application Server. Datenbank Server. Alles, was man so erwarten würde.



Ich versuche alle, auch die neuesten Schwachstellen bei deren Geräten anzugreifen. Zumindest das Medien-Plugin sollte eine offene Tür für mich sein!

Ich muss allerdings feststellen, dass anscheinend alle Rechner bei MFG mit den neusten Patches ausgestattet sind. Sowohl Betriebssystem als auch Browser Plugins sind alle auf dem neusten Stand!

Zum Geier! Alle Patches eingespielt? Selbst meine eigenen Rechner sind nicht so gut auf Stand!

Wer immer auf die MFG Endgeräte aufpasst – ist aufmerksam wie ein Dobermann und fleißig wie ein Eichhörnchen. Ich weiß es noch nicht, aber ich habe eine Gegenspielerin.

IBM

Obwohl ich noch nichts von meiner Gegnerin weiß, packt mich jetzt erst so richtig der Ehrgeiz. Ich grabe tiefer im Web und hoppla … „Schau an, wer da einen Firmen-eigenen Appstore betreibt!“

MFG Service Apps

MFG Quickfinder

Die eine lädt hoch.

Der andere runter.

MFG Side Effects Evaluator

MFG Supply

Im modernen Boxring des Digitalzeitalters sind die Ecken der Kontrahenten manchmal ziemlich weit auseinander.

Sehr servicefreundlich die IT Abteilung von MFG. Aber jetzt bin ich wieder zuversichtlich, was meine Chancen angeht. Die wenigsten wissen: Apps sind mindestens ein ebenso großes Risiko, wie eine Website!

Ich schaue mir den Sourcecode einer MFG App an. Man verwendet eine bekannte Library. Sehr schön! Wäre doch gelacht, wenn es dazu keinen Exploit gäbe!

Quickfinder

Sourcemon

Made with
MEDTRACE
SDK
©2015

CODE

GUNS

Credit Cards

DRUGS

Runterladen. Starten. Heutzutage ist alles vernetzt. Schon nimmt die App Kontakt zum MFG Mutterschiff auf. Und mein Exploit schickt ein paar blinde Passagiere mit.

„Wer öffentlich verbreitete Libraries herstellt, in Umlauf bringt oder dabei hilft, sie in Umlauf zu bringen, wird mit Sicherheitslücken nicht unter Administratorrechten bestraft“, murmele ich, als ich mir im Darkweb einen entsprechenden Exploit besorge.

„Lasset die Daten zu mir kommen!“, denke ich. Aber nix kommt. Als ob man einen Bumerang gegen einen Fliegenfänger wirft. Das würde ja heißen …

BEGIN
PATCHES
ACCESS
ATION

… Ich schaue in den Source Code. Der Patch gegen meinen Exploit ist tatsächlich schon drin. DAS KANN NICHT SEIN! Kein Entwickler ist derart vorsichtig und kennt so aktuelle Schwachstellen!

Die MFG App ist noch keine zwei Wochen alt. Und die Firma wirkte nicht so, als hätten sie eine eigene IT Security.

Appscan Ratings
13%
9%
12%

Da müssen hinter der unscheinbaren Fassade Dutzende von Leuten jede Zeile Code checken!

IBM

Nach Null-Ergebnis Brute Force und Raffinesse kommt Social Engineering. Ich muss um`s Verplatzen rausfinden, wer mir das Ausüben der ehrbahren Hacker-Profession vermiesen will. Jenny? Jenny Wer?

Da haben wir sie.

Jenny Dextra.

Urlaubsfotos und Lieblings-Smoothies.

Wenn das nicht mal eine denkwürdige Materie ist?

Kiwi is Best! Served where it grows

Input für eine neue App in Jennys Leben.

Die App tut, was sie soll. Sie verweist auf eine HTML Seite mit guten Smoothie-Rezepten.

Ein kleiner Snack fällt mit der Geburtsstunde einer App zusammen: Der Smoothie-Ratgeber. Ich schicke Jenny über Linked In einen Verweis auf die App. Aus irgendeinem Grund unter dem Nickname „Smoothie-Operator“.

Bloß liegt dahinter noch ein weiteres, verstecktes Dokument mit einer Drive-By-Infection. In dem Moment, in dem Jenny Rezepte studiert, gehört ihr Handy mir!

Sie hat angebissen! Wie kann jemand, der beruflich so Sicherheitsbewusst ist, so unvorsichtig sein.

Ist das Naivität oder Selbstbewusstsein? Voller Vorfreude mache ich mich daran, auf ihrem Handy nach dem Rechten zu sehen.

Der Smoothie, den ich auf Jennys Handy finde, hat allerdings null Vitamine. Alles nur Standard-Inhalte. Es dauert eine Weile, bis ich merke, dass ich mich in einer gekapselten Handy-Betriebssystem-Umgebung befinde.

Hurra - ich hab die Kontrolle über einen leeren Safe. Ich bin der König der Wüste Gobi. So langsam kriege ich eine Ahnung, warum sie es sich leisten kann, eine App einfach mal auszuprobieren.

Irgendwie ist ihr Handy wohl auch in die Sicherheits-abschirmung von MFG eingebunden. Die Dinger sind normalerweise so sperrangelweit offen wie die Website eines Kaninchenzüchtervereins. Ich muss unbedingt herausfinden, wie MFG das macht.

IBM

Jetzt werde ich aus einer ganz anderen Richtung kommen. Hemd, Anzug, einnehmendes Lächeln. Wenn meine Mutter mich jetzt nur sehen könnte.

MFG Health Invitation

MFG veranstaltet natürlich Kongresse. Was wäre man, ohne Business Partner? Und man möchte gar nicht glauben, wie einfach es in Zeiten schrumpfender Besucherzahlen ist, über die Event-Seite unter falschem Namen an eine Einladung zu kommen.

Ich bin jetzt Doktorand. Aber der freundliche junge Mann mit Interesse an der Health-Industrie wird nicht lange existieren. Schließlich bin ich hier, um andere Identitäten zu sammeln. Mail Adressen, Passworte … alles, was so anfällt.

MFG Health

MFG Health

MFG Health

MFG scheint ein ganz cooler Laden zu sein. Ich mache auf Konversation. Lerne viele Namen. Bin aufmerksam. Lernbegierig. „Ach … so machen die das mit ihrem Newsletter? Und der Partner-Service ist exzellent?“

Log - In

***___

Ich streife herum und filme heimlich Logins. Ein paar sind Müll, aber drei unterschiedlich privilegierte Partnerzugänge sind dabei. Noch kein Großwild, aber ein paar ausgewachsene Gazellen.

Die Bösen draußen halten und die Guten rein lassen. Dieser Filter funktioniert nicht mehr. Denn jetzt bin ich einer von den Guten!

Wieder im beruhigend vertrauten Zimmer mache ich mich ans Werk und probiere die Zugänge aus. Ich komme zwar an die Daten der Business Partner, aber das ist alles C-Ware. Und egal, welche der geklauten Accounts ich versuche – ich komme nicht aus deren Bereichen raus!

Anscheinend haben die bei MFG eine über alle Systeme genau arbeitende Rechteverwaltung, die sich aus der Identität des eingeloggten Benutzers ableitet.

Übersprünge auf nicht geregelte Verzeichnisse oder Datenbanken funktionieren nicht. Ich muss mir schon wieder was Neues einfallen lassen, während mein Auftraggeber langsam ungeduldig wird.

IBM

Ich muss fokussieren. Mich wieder auf das Wesentliche konzentrieren. Ich will an die Patientendaten ran. Und wo sind Daten im Allgemeinen? In Datenbanken. Ich probiere nochmal die ganzen Partner-Accounts durch – diesmal aber ganz genau.

Und da – beim Zweiten finde ich, was ich suche. Ein Eingabe-Formular. Ist bestimmt indirekt mit einer SQL Datenbank verbunden.

Man möchte gar nicht meinen, wie so ein SQL Server mitunter reagiert, wenn man ihn mit ein paar Sonderzeichen oder einem Overflow konfrontiert.

Also versuche ich ein paar neue SQL Injects.

Das Abfrageformular gibt anscheinend SQL Daten direkt über den Web-Application Server zum SQL Interpreter durch. Ich muss nur einen älteren SQL Server finden.

Dann kann ich mich aus der Businesspartner-Datenbank in interessantere Gefilde vortasten.

Ich kriege aber keine Infos über die verwendete SQL Version zurück. XP_cmdshell geht nicht. Benchmark-Funktionen werden für mich nicht unterstützt.

Die Daten, die ich direkt lesen kann, sind verschlüsselt. Ich versuche Unicode-Zeichen. Ich versuche, Code als Datensatz zu speichern. Ich versuche „Select into outfile“.

Egal an welchen Ecken ich versuche, Records zu ändern oder meinen Zugriff auf andere Datenbanken zu erweitern. Ich pralle ab, wie ein Wattebällchen an einer Betonwand.

Irgend eine Art von Aktivitäten-Monitor überwacht anscheinend die Integrität aller Datenbanken und die Autorisierung aller Zugriffe auf einzelne Records.

Schon wieder wasserdicht, das Ganze!

Diese Jenny ist entweder ein Genie oder sie war mal Hackerin. Und so, wie meine Versuche abgewehrt werden, ist ihre Verteidigung automatisch. Ich muss langsam wirklich ganz tief in die Trickkiste greifen!

IBM

Ich packe jetzt dickeres Werkzeug aus! Ich komme vielleicht nicht direkt an die Patientendaten. Aber ich kann mal kräftig an der Käfigtür von MFG rütteln.

Zum Glück haben die Stadtwerke Arbeitsklamotten, die man per Versand bestellen kann und Generalschlüssel für ihre Schaltkästen.

Ich finde bei MFG um die Ecke den richtigen Kasten und lege mir einen Fernschalter.

Ab jetzt gehört zumindest ein Teil der Energieversorgung ihres Serverraums mir. Dann wollen wir mal ein bisschen Energie sparen!

Ich schalte dem MFG Hauptserver den Strom ab. Befriedigt sehe ich den erhofften 404er.

ERROR 404

Aber ein Augenzwinkern später ist der Server wieder da. Zu meinem völligen Erstaunen funktioniert alles. Nicht mal die Homepage ist weg!

ACTIVE
XXX.102.0.1
XXX.101.3.100
XXX.5.7.171
MFGHealthcare

Ich krieg nen mittelschweren Wutanfall. Es ist unelegant genug, solche brachialen Methoden anzuwenden. Aber damit auch noch zu scheitern, ist beschämend!

Ich versuche, herauszufinden, warum der Server wieder da ist, obwohl ich ihm definitiv den Saft abgedreht habe. Könnte das eine Art automatischer Backup-Server sein?

ALERT

Als ich das teste, versucht jemand mit „Traceroute“ und „Finger“ herauszufinden, wer ich bin.

Natürlich kann meine Attacke nicht unbemerkt geblieben sein, aber diesmal ist Jenny mir echt auf den Fersen!

IBM

Wenn die MFG Systeme so gesichert sind, muss ich irgendwie anders an Jenny rankommen. Vielleicht ist sie bereit, mir die Daten zu geben, wenn ich Druck ausüben kann.

215 Sasdasdsadf
3,072 Sasdasdsadf
412 Sasdasdsadf

Jenny Dextra

Follow

Ascösdfösdf, Osadnlaskd

Ascösdfösdfnlaskd

JD

In den sozialen Netzwerken findet man fast alles. Klassentreffen.Verwandte. Eltern. Ich picke mir die Mutter raus, weil sie schon etwas älter ist.

BD

B. Drumb wrote:

Class of '85
Klassentreffen

Ich rufe sie an und gebe mich als ein alter Schulfreund von Jenny aus, der ihr vom Klassentreffen noch den Überschuss vom Getränkekauf überweisen muss. Bei welcher Bank war sie nochmal?

Klar frage ich nicht nach der Konto-Nummer. Aber ich erfahre den Namen der Bank und ihres „netten" Sachbearbeiters. Cool. Ich baue mir nun eine Seite, die genau so aussieht, wie die ihrer Bank – nur mit ein bisschen nagelneuem Schadcode als Zugabe.

HOME-E-BANK

Hi Jenny,

SEND

Dann schicke ich ihr eine Mail – von einem echten, bekannten Bankangestellten – mit der Bitte, über eine verlinkte Seite die neuen Nutzungsbedingungen zu bestätigen.

Diesmal muss es funktionieren! Sie hat keine Chance, zu erkennen, dass irgendetwas an dieser Mail nicht stimmt. Ich warte – meinen Bildschirm im Blick, wie ein Angler, der auf seinen Schwimmer schaut.

Zähe Stunden vergehen. Nichts rührt sich. Ich weiß, dass sie die Mail bekommen hat. Ich rufe nochmal bei der Mutter an, merke aber sofort an der Stimme, dass ich aufgeflogen bin.

Comments:

JD

JD Posted:
NICE TRY!!!

Leave a Reply

Comment

Meine Fake-Bank-Page bleibt natürlich verwaist. Allerdings nicht ganz, wie ich merke, als ich einen Refresh mache und einen Eintrag in einem Kommentarfeld bemerke.

Post Comment

Call MOM

Anscheinend hat das System von MFG gemerkt, dass die Bank-Seite nicht von der IP-Adresse des Bankservers kam. Mein Fishing ist ins Leere gelaufen. Und eine Mutter kriegt bestimmt Nachhilfe-Unterricht für das Digitalzeitalter.

IBM

Am Ende mit dem Latein! Ich selber weiß jetzt nur noch einen Weg. Ich stelle ein Dossier mit allem zusammen, was ich bislang über die Systeme von MFG gesammelt habe …

… und platziere selber einen Job im Darknet. Ich suche einen Programmierer, der mir maschinennah einen spezifischen Exploit für das Netz von MFG erstellt. Dagegen gibt es keinen Schutz!

Die Beauftragung eines anonymen Programmierers aus Osteuropa frisst alles auf, was ich an Honorar überhaupt für den Hack zu erwarten habe. Aber mir bleibt keine andere Wahl!

Voller Ungeduld warte ich auf meine Lieferung. Dann – endlich ist sie da.

Ich starte alle Komponenten so, wie mein unbekannter Kollege mir das vorschreibt. Und endlich bin ich drin bei MFG. Shell-Ebene. Admin-Rechte.

Weil vorher so viel schiefgegangen ist beeile ich mich und kopiere die Patienten-Akten-Datenbank auf meine Platte. Dann logge ich aus.

Sieg. Endlich! Ich schaue in einige Datensätze rein. Und denke, mich tritt ein Pferd. Verschlüsselt, Ich muss noch die Keys dazu aus dem MFG Netz kopieren.

Mein maßgeschneiderter Exploit ist gerade erst Stunden alt. Ich muss nochmal bei MFG rein! Ich mache alles wie eben und pralle ab! Und das ist der Moment, in dem ich mir meine Niederlage eingestehen muss

Diese schnelle Abwehr kann unmöglich Jennys Werk sein. Offenbar ist da ein heuristisches System am Werk, dass Angriffe analysieren kann, die es so vorher noch nicht gab.

„Und das ist, soweit ich die Geschichte erzählen kann.

Das ist natürlich nicht das Ende. Ich weiß nicht ob das Rennen zwischen den Adams und den Jennys dieser Welt je entschieden wird.

Ich weiß nicht, ob die Verletzbarkeit unserer Systeme jemals wieder anfängt, kleiner zu werden oder ob wir alle irgendwann so von Sicherheitsmaßnahmen überladen werden, dass wir wieder zu Papier und Stift übergehen.

Ich weiß nur, dass wer immer Jenny geholfen hat, ihren Job zu machen, wirklich sehr gute und umfassende Sicherheitslösungen am Start hat….

IBM