

Trotz mehrfacher Hinweise (über Wochen) auf eine Schwachstelle in den VZ-Netzwerken, haben die Betreiber bis heute nicht ausreichend reagiert und das System ausgebessert.

Die Schwachstelle birgt die Möglichkeit eMails an beliebige Nutzer der Community zu versenden, die nachweislich von einem offiziellen Server der VZ Netzwerke stammen. Dies klingt zunächst nicht dramatisch. Allerdings ist es möglich, bestimmte Textabschnitte in der eMail frei zu bestimmen. Als Folge dessen ist es möglich unbedarfte Benutzer auf eine manipulierte Webseite zu locken und sie dort dazu zu bringen ihre Zugangsdaten preiszugeben.

Angreifbar ist das System durch eine Funktionalität („Einem Freund zeigen“) auf der Seite, mit der es möglich ist, ausgewählte Seiten per eMail an Freunde zu schicken. Dies ist z.B. unter dem Link „Jobs“ möglich, der sich im unteren Bereich (Footer) der VZ Seite befindet:



Folgt man diesem Link, so gelangt man zu den aktuellen Jobangeboten der VZ Netzwerke. Interessanter ist allerdings der Link, der im oberen rechten Teil der Seite angezeigt wird:



Dies ist die gerade beschriebene Funktionalität, mit der man einem VZ-Freund auf diese Seite verweisen kann. Nach einem Klick auf diesen Link öffnet sich eine neue Seite.



MEINVERZEICHNIS English Suche Einladen Hilfe Klartext Handy Blog Raus hier

Das Fundstück Deinen Freunden zeigen Röhre Plauderkasten (0)

Zeige das Fundstück Deinen Freunden im meinVZ oder auch Leuten, die noch nicht registriert sind.

Übrigens: Innerhalb der VZ-Netzwerke kannst Du einen Inhalt immer nur den Leuten auf einer Deiner Freundeslisten und max. zehn weiteren Freunden zeigen.

An [\[Adressbuch checken\]](#)

Betreff noch 38 Zeichen

Hinweis: Es kann vorkommen, dass aufgrund von Sichtbarkeits-Einstellungen nicht alle Empfänger das Gezeigte sehen können. (z.B. wenn der Besitzer eines Fotos dieses nur für seine Freunde freigegeben hat).

Betrachtet man die URL zu dieser Seite, zeigt sich dass sie einen Parameter „u“ enthält, der die Seite spezifiziert, die man seinem VZ-Freund zeigen möchte.

<http://www.meinvz.net/Link/ExternLink/Url/?u=http%3A%2F%2Fwww.meinvz.net%2Fstart&desc=xxx.+möchte+Dir+eine+Seite+zeigen!&prov=meinVZ>

Dieser Parameter war bis vor kurzem noch vollständig manipulierbar. Hier konnte beliebiger Text eingefügt werden. Nach den ersten Hinweisen an die Betreiber wurde dieser Parameter dahingehend verbessert, als dass er mindestens folgenden Text enthalten muss: <http://www>

Dies ist natürlich nicht ausreichend und wurde dem Betreiber auch mitgeteilt. Folgendes Szenario zeigt wo die Gefährlichkeit dieses Parameters besteht:

Ein potenzieller Angreifer könnte hier folgende URL einbetten:

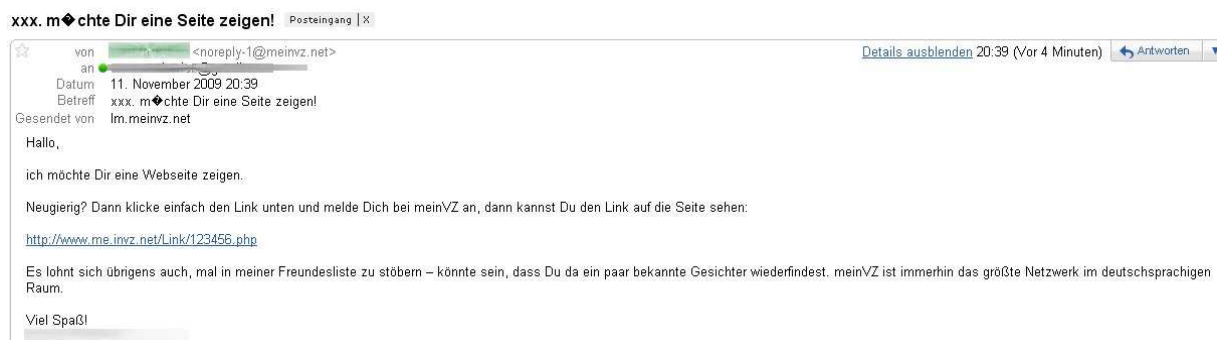
<http://www.me.invz.net/Link/123456.php>

Studiert man diese URL genauer, fällt auf, dass sie aus folgenden Elementen besteht:

Domain: invz.net

Sub-Domain: me

Die vom VZ-System verschickte eMail sieht in diesem Fall folgendermaßen aus:



Der manipulierte Link wurde also unverändert in die eMail übernommen. Desweiteren kann man im Feld „Gesendet von“ sehen, dass die eMail von einem offiziellen VZ-Server gesendet wurde.

Gesendet von Im.meinvz.net

Im Absenderfeld „von“ taucht der Benutzername auf, von dem aus man den Link verschickt hat.

Der Empfänger dieser eMail auf Grund der Tatsachen, die auf eine offizielle Nachricht der VZ Community schließen lassen, einfach übersehen, dass die URL nicht auf eine Seite innerhalb der VZ Netzwerke verweist. Ein Angreifer könnte nun unter der Adresse des manipulierten Links eine Nachbildung einer VZ Seite hinterlegen, die z.B. so aussieht:



Hauptseite
Einloggen
Registrieren

Die Fußballwelt trauert um Robert Enke.

MEINVERZEICHNIS English Registrieren Hilfe Klartext Handy Blog

Einloggen

Falsche E-Mail-Adresse oder falsches Passwort!

E-Mail:

Passwort:

Eingeloggt bleiben ?

Sitzung sichern ?

[Passwort vergessen?](#)
[E-Mail - Aktivierungslink noch einmal zusenden](#)

Über uns	AGB	Regionen
Presse	Datenschutz	Edelprofile
Jobs	Impressum	Politikerprofile
Sicherheit	Verhaltenskodex	Entwickler
Tipps	Werbung	

DsiN.de DEUTSCHLAND SICHER IM NETZ

fsm ORIGINALER HINLEITER

VZ-Datenschutz Deine Daten gehören Dir.

Der User wird in diesem Fall sehr wahrscheinlich keinen Verdacht schöpfen, und seine Zugangsdaten (eMailadresse und Passwort) eingeben. Die angezeigte Seite könnte die Daten auswerten und an den Angreifer senden, der dann sofort die Kontrolle über den Account des Opfers übernehmen kann. Um weniger Verdacht aufkommen zu lassen, könnte er die Seite auch so programmieren, dass sie das Opfer auf die originale VZ Seite weiterleitet.

Wenn der Angreifer noch einen Schritt weiter gehen will, so kann er bevor er den Einladungslink verschicken lässt, auch noch seinen Benutzernamen ändern. Ein Beispiel wäre hier:

Vorname = MeinVZ

Nachname = Zentrale

Dies hat den Vorteil, dass die eMail mit dem Einladungslink nun noch authentischer aussieht. Sie wirkt nun, als wäre sie direkt vom VZ System verschickt worden, denn im Absenderfeld taucht der Name „MeinVZ Zentrale“ auf. Diesen Absender haben auch offizielle eMails, die man von den VZ Netzwerken gesendet bekommt.

MeinVZ Zentrale möchte Dir eine Seite zeigen! Posteingang | X

von **MeinVZ Zentrale** <noreply-1@meinvz.net> [Details ausblenden](#) 20:57 (Vor 3 Minuten) [Antworten](#)

an [\[Name\]](#)

Datum 11. November 2009 20:57

Betreff MeinVZ Zentrale möchte Dir eine Seite zeigen!

Gesendet von lm.meinvz.net

Hallo,

ich möchte Dir eine Webseite zeigen.

Neugierig? Dann klicke einfach den Link unten und melde Dich bei meinVZ an, dann kannst Du den Link auf die Seite sehen:

<http://www.meinvz.net/Link/123456.php>

Es lohnt sich übrigens auch, mal in meiner Freundesliste zu stöbern – könnte sein, dass Du da ein paar bekannte Gesichter wiederfindest. meinVZ ist immerhin das größte Netzwerk im deutschsprachigen Raum.

Viel Spaß!
MeinVZ Zentrale

