Analyse

Verschlüsselte Kontaktaufnahme auf der Webseite der Stadt Mettmann

von Ralf Krüdewagen
Mitglied der Piratenpartei Deutschland
Sachkundiger Bürger im Bürgerausschuss der Stadt Mettmann

Version 0.21 vom 07.09.2014

Hintergrund

Diese Analyse bezieht sich auf die Bürgeranregung gem. § 24 Gemeindeordnung Nordrhein-Westfalen zur „**Sicherheit der kommunalen IT-Infrastruktur**“, die die Piraten in Mettmann bei der Stadtverwaltung Mettmann am 05.05.2014 eingereicht haben.

Diese Bürgeranregung wurde mittlerweile von der Verwaltung erläutert und dem Verwaltungsausschuss zur 2. Sitzung am 02.09.2014 als Informationsvorlage vorgelegt.

Die Dokumente zur 2. Sitzung des Verwaltungsausschusses mit Vorlagen und Anlagen finden sich hier:

http://offene-daten.me/dataset/2-sitzung-des-verwaltungsausschusses

http://offene-daten.me/dataset/2-sitzung-des-verwaltungsausschusses/resource/60999ff7-e3a3-4b3d-a6ad-9b6d5fb3b136

In dieser Analyse möchte ich vor allem auf **Punkt 7** dieser Bürgeranregung eingehen.

> *Frage:*
>
> *7. Warum bietet die Gemeinde Mettmann auf ihrer Kontaktseite im Internet keine Möglichkeit für den Bürger zu einer verschlüsselten Kontaktaufnahme?*
>
> *Verwaltungserläuterung:*
>
> *Inzwischen steht auf www.mettmann.de die Möglichkeit zur verschlüsselten Kontaktaufnahme zur Verfügung.*

Gegenstand dieser Analyse ist es, diese Möglichkeit zur verschlüsselten Kontaktaufnahme auf der Webseite http://www.mettmann.de zu überprüfen.

Voraussetzungen und Annahmen

Meine Untersuchungen basieren ausschließlich auf einer Überprüfung „von außen“, wie sie jeder Sachkundige ohne Kenntnis von Interna der beteiligten IT-Systeme ebenfalls vornehmen kann. Ich habe weder Einsicht in die beteiligten Internetknoten und Server oder deren interne Konfiguration, noch habe ich Zugang zu den serverseitigen Quellen der Webanwendung der Stadt Mettmann.

In einigen Punkten muss ich daher bestmögliche Annahmen treffen, die ich jeweils kennzeichne. Die zentrale Annahme betrifft den Weitertransport der Daten vom Webserver zum Rechenzentrum der Stadt Mettmann per E-Mail. Leider kann ich „von außen“ keine andere Annahme treffen.

Ergebnis

Da die Verwaltung keine näheren Angaben gemacht hat, wie und wo die verschlüsselten Kontaktaufnahme auf der Webseite http://www.mettmann.de implementiert wurde, habe ich einige Minuten benötigt, um herauszufinden, was damit gemeint ist.

Das einzige, was man aus meiner Sicht gemacht hat: Man hat das Feedbackformular unter "*Aktuelles & Kontakte -> Feedbackformular*" so gestaltet, dass automatisch von der unverschlüsselten (*http://*) auf die verschlüsselte (*https://*) Seite der Stadt Mettmann weitergeleitet wird.

Der Link http://www.mettmann.de/service/feedback.php wird also nach https://www.mettmann.de/service/feedback.php weitergeleitet.

Das bedeutet, dass die Daten, die der Besucher in das Feedbackformular einträgt, zwischen Client (Browser) und Server (Webseite) verschlüsselt werden. Diese Verschlüsselung ist auf dem Stand der Technik (siehe technischen Analyse unten) und ein erster richtiger und wichtiger Schritt.

Allerdings ist diese Verschlüsselung zwischen Browser und Webseite allein nicht ausreichend bzw. nicht zu Ende gedacht, wie die weitere Untersuchung ergibt.

Nachdem der Webserver der Stadt Mettmann die Daten nämlich aus dem Feedbackformular angenommen hat, müssen diese Daten weiterverarbeitet werden. Aus der technischen Analyse ergibt sich, dass die Daten im nächsten Schritt **unverschlüsselt per E-Mail durch das Internet** geschickt werden.

Dieser Umstand erklärt sich daraus, dass der Webserver der Stadt Mettmann bei einem externen Webhoster (Host Europe) steht und der Annahme, dass die Daten dann in das Rechenzentrum der Stadt Mettmann per E-Mail übertragen werden, damit diese dort von Mitarbeitern der Stadt eingesehen und bearbeitet werden können.

Bei der dabei eingesetzte Weiterleitung der Daten per E-Mail wird in unserem Fall jedoch keine Transportverschlüsselung angewandt. Von

Transportverschlüsselung redet man, wenn die Daten, die zwischen zwei IT-Rechnersystemen ausgetauscht werden, auf dem Transportweg verschlüsselt werden. Dabei werden die Daten auf jedem beteiligten Knoten kurz entschlüsselt und dann wieder für den nächsten Knoten der Kommunikationskette verschlüsselt. Auf der Leitung selbst sieht ein Beobachter oder Angreifer jeweils nur verschlüsselte Daten.

Wenn diese Transportverschlüsselung nicht stattfindet, ergibt sich folgendes Risiko: Die Daten können durch Anzapfen von Leitungen bei den jeweiligen Providern oder bei den Netz-Zusammenschaltpunkten des Internetverkehrs (z.B. DE-CIX) ohne große Probleme mitgelesen werden. Und wie man mittlerweile weiß: Genau das geschieht flächendeckend.

Zumindest auf dieser Transportebene sollte daher eine durchgehende Verschlüsselung stattfinden, wobei Sender und Empfänger entsprechend ausgerüstet werden müssen und das auch getestet werden muss. Das ist Stand der Technik und i.d.R. bei aktuellen Systemen ohne Mehrkosten recht einfach einzurichten. Das geschieht aber im Fall der Stadt Mettmann eben nicht und darf aus technischer Sicht und mit dem heutigen Wissen als grob fahrlässig angesehen werden!

Von daher stimmt es nicht, dass eine verschlüsselten Kontaktaufnahme möglich ist!

Anmerkung 1:

Im übrigens ist von dieser Schwachstelle nicht nur das Feedbackformular betroffen, sondern – soweit ich es erkennen kann – alle Online-Formulare der Stadt Mettmann, so z.B. das Bestellformular für Restmülltonnen https://www.mettmann.de/abfallberatung/formulare/form_restmuell.php. Hier ist die Lage sogar noch kritischer, da gezielt personenbezogene Daten abgefragt werden wie z.B. Name, Kassenzeichen, etc.

Zudem betrifft die Schwachstelle alle eingehenden E-Mails an die Domain „mettmann.de“. Sämtliche E-Mailkommunikation zu E-Mail-Adressen der Stadt Mettmann wird auf dem Transportweg nicht ausreichend nach Stand der Technik geschützt.

Anmerkung 2:

Selbst im Fall einer durchgehenden Transportverschlüsselung (von Knoten zu Knoten) wäre die Verschlüsselung aber nicht Ende-zu-Ende. Denn die Daten aus dem Feedbackformular liegen als unverschlüsselte E-Mails zunächst kurz beim externen Webhoster und dann im Rechenzentrum der Stadt Mettmann vor. Für den Fall einer echten Ende-zu-Ende Verschlüsselung wäre eine zusätzliche Verschlüsselung der E-Mails an der Quelle mittels S/MIME und PGP nötig.

Technische Analyse

a) Verschlüsselung der Webseite

Das Feedbackformular https://www.mettmann.de/service/feedback.php wird nach einer Weiterleitung von HTTP nach HTTPS verschlüsselt. Die Daten werden also vom Rechner des Besuchers zum Webserver verschlüsselt. Eine Analyse der SSL/TLS-Verschlüsselung ergibt, dass sogar Forwards Secrecy

eingerichtet ist:

```
~> openssl s_client -connect www.mettmann.de:443|grep Cipher

New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA
    Cipher    : DHE-RSA-AES256-SHA
```

Fazit: Die Webseite verwendet mit DHE-RSA-AES256-SHA einen sicheren Cipher nach Stand der Technik. Sehr gut.

b) Datenweiterleitung aus dem Formular

Der Webserver steht laut IP-Adresse 83.169.31.74 bei Host Europe GmbH mit Sitz in Köln:

```
~> nslookup www.mettmann.de
Name:   www.mettmann.de
Address: 83.169.31.74

~> whois 83.169.31.74
inetnum:        83.169.24.0 - 83.169.31.255
remarks:        INFRA-AW
netname:        DE-HE-SH-WPPRO-CGN32-NET
descr:          Host Europe GmbH
descr:          hostmaster@hosteurope.de
country:        DE
admin-c:        HER
tech-c:         HER
status:         ASSIGNED PA
mnt-by:         HOSTEUROPE-MNT
source:         RIPE # Filtered

role:           Host Europe Ripehandle
address:        Welserstrasse 14
address:        51149 Koeln
```

Das Formular verwendet zur Weiterverarbeitung der eingegebenen Daten einen HTTP POST mit dem Ziel „/mailer/feedback.php“. Das legt den Schluss nahe, dass die Daten per E-Mail an die Stadtverwaltung Mettmann weitergeleitet werden. Ich nehme an, an eine E-Mail Adresse unter der Domain *mettmann.de*.

Es wäre theoretisch auch möglich, die E-Mails auf dem Webserver zu belassen und dort zur Abholung per IMAP anzubieten. Auf dem Webserver läuft nämlich auch ein IMAP-Mailserver, der sogar Verschlüsselung (STARTTLS) anbietet:

```
~> telnet www.mettmann.de 143
Trying 83.169.31.74...
Connected to www.mettmann.de.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE STARTTLS
AUTH=PLAIN AUTH=LOGIN] Dovecot ready.
```

Allerdings ist der Webserver nicht offiziell für E-Mails an *@mettmann.de* zuständig. Und auch eine Analyse des TLS-Zertifikats ergibt, dass es sich sehr wahrscheinlich um ein Standard-Zertifikat von Host Europe handelt:

```
~> openssl s_client -starttls imap -connect www.mettmann.de:143
CONNECTED(00000003)
depth=2 C = BE, O = GlobalSign nv-sa, OU = Root CA, CN = GlobalSign Root CA
verify return:1
depth=1 C = BE, O = GlobalSign nv-sa, CN = GlobalSign Organization Validation
CA - G2
verify return:1
depth=0 C = DE, ST = Nordrhein-Westfalen, L = Koeln, O = Host Europe GmbH, CN
= *.webpack.hosteurope.de
verify return:1
---
Certificate chain
 0 s:/C=DE/ST=Nordrhein-Westfalen/L=Koeln/O=Host Europe
GmbH/CN=*.webpack.hosteurope.de
   i:/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Organization Validation CA - G2
 1 s:/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Organization Validation CA - G2
   i:/C=BE/O=GlobalSign nv-sa/OU=Root CA/CN=GlobalSign Root CA
```

Man kann nun hergehen und schauen, wohin E-Mails an *@mettmann.de* gehen (MX Record im DNS):

```
~> nslookup
> set type=mx
> mettmann.de
Non-authoritative answer:
mettmann.de     mail exchanger = 10 barracuda.mettmann.de.

~> nslookup barracuda mettmann.de
Name:   barracuda mettmann.de
Address: 195.145.217.5
```

Die E-Mails gehen also zu *barracuda.mettmann.de* mit der IP 195.145.217.5, welche von der Deutsche Telekom AG an den Kreis Mettmann zugeteilt ist:

```
~> whois 195.145.217.5
inetnum:        195.145.216.0 - 195.145.219.255
netname:        KME
descr:          Kreisverwaltung Mettmann
descr:          D-40822 Mettmann
country:        DE
admin-c:        RG620-RIPE
tech-c:         RG620-RIPE
status:         ASSIGNED PA
mnt-by:         DTAG-NIC
source:         RIPE # Filtered

person:         Rene Gruen
address:        Sg. 10-35
address:        Kreisverwaltung Mettmann
address:        Duesseldorfer Str. 26
address:        D-40822 Mettmann
```

Dies scheinen IP-Adressen zu sein aus dem besagten Rechenzentrum.

Fazit: Die von den Besuchern im Formular eingegebene Daten werden als normale E-Mails zwischen zwei Providern über das Internet ausgetauscht, wobei der Webserver für *mettmann.de* bei einem anderen Provider steht als der Mailserver für *mettmann.de*.

c) Transport der E-Mails

Als nächstes schaut man sich an, wie *barracuda.mettmann.de* E-Mails entgegen nimmt. Und man stellt fest, dass dieser Mailserver beim Kreis Mettmann keine Verschlüsselung auf Transportebene unterstützt (STARTTLS).

```
~> openssl s_client -starttls smtp -connect barracuda.mettmann.de:25|grep
Cipher

didn't found starttls in server response, try anyway...

139672666699408:error:140790E5:SSL routines:SSL23_WRITE:ssl handshake
failure:s23_lib.c:184:

New, (NONE), Cipher is (NONE)
```

Eine verschlüsselte Verbindung würde man so erkennen:

```
~> openssl s_client -starttls smtp -connect smtp.1und1.de:25|grep Cipher

New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES256-GCM-SHA384

    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
```

Fazit: Die Mails mit den Daten von der Mettmanner Homepage gehen **unverschlüsselt** auf die Reise durchs Internet zwischen den beiden Providern.

Fazit

Eine verschlüsselte Kontaktaufnahme ist auf der Webseite der Stadt Mettmann nicht wirklich möglich. Es wird lediglich der Verkehr zwischen Browser und Webserver verschlüsselt. Tatsächlich findet die Kommunikation im Hintergrund über ungesicherte und unverschlüsselte Kanäle statt.

Ich empfehle dringend, eine Transportverschlüsselung (SSL/TLS) der beteiligten Netzelemente einzurichten. Hier ist besonderes Augenmerk auf den für die Domain *mettmann.de* zuständigen Mailserver zu richten.

Datenschutzrechtlicher Exkurs

Bei der Analyse der Webseite http://www.mettmann.de sind mir ad-hoc zwei datenschutzrechtlich relevante Dinge aufgefallen. Aus datenschutzrechtlicher Sicht kann die Webseite der Stadt Mettmann daher aus meiner Sicht als rechtswidrig angesehen werden.

1. Tracking der Besucher

Die Webseite setzt aktives Tracking der Besucher ein. Dieses Tracking wird mit der Open Source Software Piwik [2] vorgenommen.

```
<!-- Piwik -->

<script type="text/javascript">

var pkBaseURL = (("https:" == document.location.protocol) ?
"https://www.mettmann.de/piwik/" : "http://www.mettmann.de/piwik/");

document.write(unescape("%3Cscript src='" + pkBaseURL + "piwik.js'
type='text/javascript'%3E%3C/script%3E"));

</script>
```

Die Daten landen auf dem Webserver selbst, was zunächst einmal löblich ist. Gegenüber einer externen Datenverarbeitung über z.B. Google Analytics zeichnet sich Piwik dadurch aus, dass damit datenschutzrechtlich weniger invasives Tracking stattfinden kann.

Allerdings gibt es **keine Datenschutzerklärung** mit dem Hinweis, was z.B. mit dabei gesammelten IP-Adressen geschieht, ob diese anonymisiert werden und ob „Do not Track“ [3] beachtet wird.

Wenigstens das Deaktivieren des Trackings ist über das Impressum möglich: http://www.mettmann.de/service/impressum.php

2. Google Suche

Man setzt Google für die lokale Suche ein. Jede Seite unter http://www.mettmann.de enthält dazu Code, der „sich mit Google-Servern unterhält“:

```
<script src="https://www.google.de/jsapi" type="text/javascript"></script>
<script type="text/javascript">
  google.load('search', '1', {language : 'de'});
  google.setOnLoadCallback(function() {
    var customSearchOptions = {};  var customSearchControl = new
google.search.CustomSearchControl(
      '007377010588224942992:fi9xikdqfsu', customSearchOptions);
    customSearchControl.setResultSetSize(google.search.Search.FILTERED_CSE_RESULTSET);
    var options = new google.search.DrawOptions();
    options.enableSearchboxOnly("http://www.mettmann.de/suchen2.php");
    customSearchControl.draw('cse-search-form', options);
  }, true);
</script>
<link rel="stylesheet" href="https://www.google.com/cse/style/look/default.css" type="text/css" />
<style type="text/css">
  input.gsc-input {
    border-color: #D9D9D9;
  }
  input.gsc-search-button {
    border-color: #cccccc;
    background-color: #cccccc;
  }
</style>
```

Damit wird nicht nur die lokale Suche über Google abgewickelt, was an sich schon sehr grenzwertig ist, sondern Google erhält auch Informationen über jede besuchte Seite der Stadt Mettmann, u.a. mit der IP-Adresse der Besucher.

Abgesehen davon, dass diese Suche lokal implementiert werden sollte, vermisse ich auch hier eine **Datenschutzerklärung**.

Quellangaben

[1] http://www.heise.de/security/artikel/Forward-Secrecy-testen-und-einrichten-1932806.html

[2] http://piwik.org

[3] https://de.wikipedia.org/wiki/Do_Not_Track

