Dirección de Ciberseguridad

Dirección Provincial de Planificación y Desarrollo TIC,
Oficina Provincial de Tecnologías de Información y Comunicaciones,
Secretaría de Modernización de Gestión Pública,
Ministerio de Cultura, Juventud, Deporte y Gobierno,
Gobierno de la Provincia del Neuquén

Implementación de NO-CAPTCHA en Outook Web Application (OWA) 2010

Los ataques de fuerza bruta contra aplicaciones Microsoft Outlook Web Application (OWA) son un caso frecuente y de larga data.

Soluciones como segundo factor de autenticación (algo que el usuario tiene, algo que el usuario es), requieren de recursos adicionales que no siempre están al alcance de los organismos.

El uso de CAPTCHA surge como una solución intermedia adonde el único esfuerzo que insume es el de su implementación propiamente dicha.

En este documento, se describen los pasos para incorporar un widget no-captcha reCAPTCHA en páginas de autenticación de Outlook Web App 2010. Se conoce como no-captcha debido a que mejora la experiencia de los Usuarios al requerir solamente tildar sobre la consulta "No soy un robot", ante los captcha tradicionales que requieren de la identificación de una imagen o texto.

Si bien esta solución no se ha verificado en versiones anteriores, como OWA 2003 o OWA 2007, se debería seguir un esquema similar.

En primer lugar, se debe generar una Clave Privada y una Clave Pública (Public Key) en el sitio de reCAPTCHA de Google:

https://developers.google.com/recaptcha

Estas claves se utilizarán en el código que se agregará en la página de Autenticación de OWA, dentro del Formulario de Autenticación (FBA), tal como se explica más adelante.

Importante: Al crear las claves, se debe especificar la URL pública del sitio OWA y luego utilizar esa misma URL en el código. Si la URL indicada al momento de la generación de las Claves es distinta a la indicada en el código, será rechazada por el servicio de reCAPTCHA.

ReCAPTCHA valida la entrada del Usuario mediante el envío de los datos al servicio de validación reCAPTCHA de Google. Se debe crear un solicitante XMLHTTPRequest (usando JavaScript) para derivar la entrada del Usuario a dicho servicio.

Aquí reside un problema, y es que XMLHTTPRequest no permite transferir datos a un sitio diferente al que carga la página actual. Esto se debe a una política de seguridad conocida como Política de Mismo Origen (Same Origin Police).

Para resolver este problema, se debe crear una nueva página en el Servidor OWA para que actúe como un proxy, y que sea ésta la que realice el envío al validador reCAPTCHA. Esta página extra devuelve un código de éxito o error a la página de autenticación de OWA, indicando si puede proceder con el inicio de sesión o no.

Para crear esta nueva página, localizar la siguiente carpeta:

C:\Program Files\Microsoft\Exchange Server\V{version X}\ClientAccess\Owa\auth folder

Crear con Bloc de Notas un nuevo archivo con el nombre **Recaptcha.aspx** y pegar el código que se presenta abajo.

Importante: Reemplazar el texto "private key" con la Clave Privada de reCAPTCHA.

```
<% @ Page AspCompat=True Language = "VB" %>
<%
' Ingresa tu Clave privada en la siguiente linea…
Dim strPrivateKey As String = "private key"
Dim strResponse = Request("response")
Dim objWinHTTP As Object
objWinHTTP = Server.CreateObject("WinHTTP.WinHTTPRequest.5.1")
objWinHTTP.Open("POST",
"https://www.google.com/recaptcha/api/siteverify", False)
objWinHTTP.SetRequestHeader("Content-type", "application/x-www-form-
urlencoded")
Dim strData As String = "secret=" & strPrivateKey & _
  "&response=" & strResponse
objWinHTTP.Send(strData)
Dim strResponseText = objWinHTTP.ResponseText
Response.Write(strResponseText)
%>
```

A continuación, realizar un backup del archive **logon.aspx**, en la misma carpeta, para preservar la versión original, dado que se introducirán algunos cambios.

Abrir el archivo **logon.aspx** con un Bloc de Notas, ubica el tag "**form action**" con el buscador (CTRL-F) y quitar la acción tal como se muestra a continuación:

```
<form action="" method="POST" name="logonForm" ENCTYPE=
```

Luego, ubicar el texto **basicExplanationContent**. Se encuentra en una línea como la que sigue:

```
                <td><%=basicExplanationContent %></td>
            </tr>
            <% } %>
        </table>
    </td>
</tr>
<% } %>
<tr><td><hr></td></tr>
```

Inmediatamente después de esa última línea, insertar el código que sigue. Notar que el valor de la Clave Pública debe ser la generada en el sitio reCAPTCHA.

```
<tr>
<td>
<script type="text/javascript">
function miClkLgn()
{
  var oReq = new XMLHttpRequest();
  var sResponse = document.getElementById("g-recaptcha-
response").value;
  var sData = "response=" + sResponse;
  oReq.open("GET", "/owa/auth/recaptcha.aspx?" + sData, false);
  oReq.send(sData);
  if (oReq.responseText.indexOf("true") != -1)
  {
    document.forms[0].action = "/owa/auth.owa";
    clkLgn();
  }
  else
  {
    alert("Respuesta CAPTCHA incorrecta!");
  }
}
</script>
<script src="https://www.google.com/recaptcha/api.js" async
defer></script>
<div class="g-recaptcha" data-sitekey="Clave Pública"></div>
</td>
</tr>
```

Localizar ahora la siguiente línea de código:

```
(Strings.IDs.LogOn) %>" onclick="clkLgn()"
```

Reemplazarla como se muestra a continuación:

```
(Strings.IDs.LogOn) %>" onclick="miClkLgn()"
```

Esto último hará que se invoque el código ingresado cuando el Usuario envíe la solicitud de autenticación.

Guardar el archivo y cerrarlo. Acceder a OWA para verificar los cambios y el funcionamiento correcto de la funcionalidad incorporada.

Se debería obtener un Formulario de Autenticación como el que se muestra a continuación en la imagen que sigue.

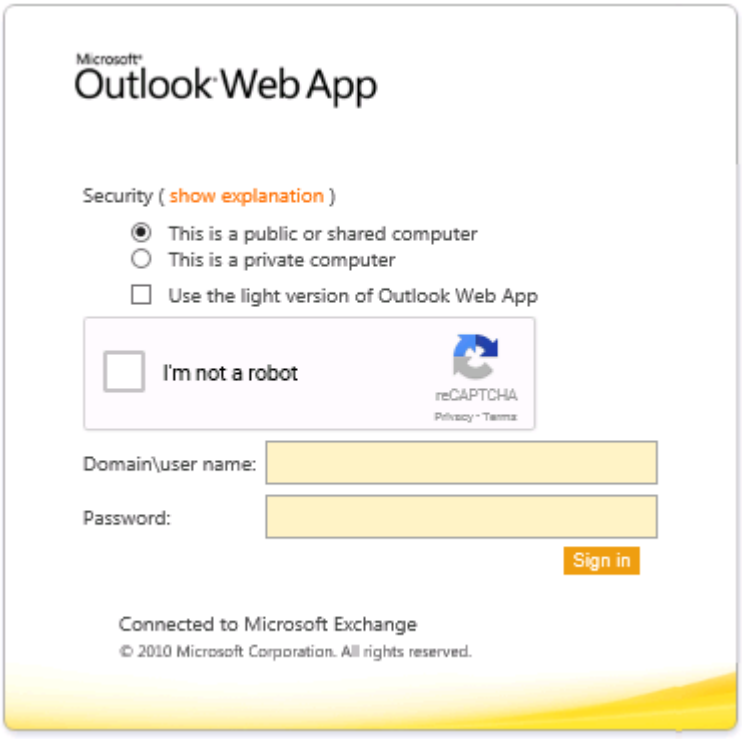

Figura 1. Implementación reCAPTCHA en Autenticación OWA 2010