blog.knowbe4.com /open-redirect-flaws-phishing-trick

Failles de redirection ouvertes et la dernière astuce de phishing

NDLR: dans le texte "Phishing" signifie: hameçonnage

Stu Sjouwerman :

Pas de surprise : les attaques de phishing sont à la hausse, et une vieille technique est de plus en plus populaire : les failles de redirection ouvertes.
Ces failles permettent aux attaquants de rediriger les victimes vers des sites Web malveillants, même si le lien dans le courriel de phishing semble légitime.

Comment fonctionnent les failles de redirection ouverte?

Les failles de redirection ouvertes se produisent lorsqu'un site Web permet aux utilisateurs de saisir leurs propres URL dans un lien de redirection.
Si le site Web ne valide pas ou ne nettoie pas correctement ces entrées, les attaquants peuvent utiliser la faille pour rediriger les victimes vers des sites Web malveillants.
Par exemple, les attaquants peuvent envoyer des courriels de phishing contenant un lien vers un site Web légitime, tel que bankofamerica.com.
Cependant, le lien pourrait en fait rediriger les destinataires vers un site malveillant qui ressemble au vrai site de Bank of America.

Pour vous protéger contre les attaques de redirection ouvertes, procédez comme suit :

1. Méfiez-vous des liens dans les courriels provenant d'expéditeurs inconnus.
2. Ne cliquez pas sur les liens dans les courriels contenant des fautes de frappe ou des erreurs grammaticales.
3. Passez la souris sur les liens dans les e-mails pour voir l'URL réelle avant de cliquer dessus.
4. Utilisez une solution de sécurité capable de détecter et de bloquer les liens de redirection ouverts.

Les organisations peuvent également prendre des mesures pour se protéger contre ces types d'attaques, par exemple en offrant aux employés une formation de sensibilisation à la sécurité sur la façon d'identifier les courriels d'ingénierie sociale et de phishing.

Voici quelques conseils supplémentaires pour reconnaître les failles de redirection ouvertes dans les e-mails de phishing :

1. Recherchez un service de raccourcissement d'URL.
   Les attaquants utilisent souvent des raccourcisseurs d'URL pour dissimuler des liens malveillants dans les courriels de phishing.
2. Examinez toujours attentivement l'URL du lien.
   S'il contient des caractères ou des paramètres étranges, il est préférable de ne pas cliquer dessus.
3. Passez la souris sur le lien avant de cliquer dessus.
   Cela vous permettra de vérifier que le lien pointe vers le site Web qu'il prétend être plutôt que vers un contenu malveillant.
4. En cas de doute, il est toujours préférable d'être prudent et d'éviter de cliquer dessus.

En éduquant les employés sur les failles de redirection ouvertes et en portant une attention particulière aux liens dans les courriels, vous pouvez réduire le risque d'être victime de ces failles dans les attaques de phishing.

La formation de sensibilisation à la sécurité de la nouvelle école peut permettre aux employés de suivre les meilleures pratiques de sécurité et d'éviter de tomber dans les pièges de l'hameçonnage et de l'ingénierie sociale.

HelpNet Security a toute l'histoire.

Recherche et mise en page:
Michel Cloutier
CIVBDL
20230906
"C'est ensemble qu'on avance"