29 Jan. 2025 -08:39

44 % der Belgier leiten Phishing-Nachrichten an suspekt@safeonweb.be weiter

Im Jahr 2024 leiteten aufmerksame Bürger mehr als 9 Millionen Nachrichten an suspekt@safeonweb.be . Im Rekordjahr 2023 waren es 10 Millionen. Im Jahr 2024 erhielten wir durchschnittlich 25.900 Nachrichten pro Tag. Wir möchten uns bei allen Internetnutzern, die dies weiterhin tun, ganz herzlich bedanken! Gemeinsam machen wir das Internet zu einem sichereren Ort.

Mit diesen Informationen konnten wir genau 1.644.732 verdächtige Links erkennen und umleiten. Weniger aufmerksame Internetnutzer, die auf einen solchen Link klicken, werden von uns auf eine Warnseite umgeleitet und somit nicht betrogen.

Eine Umfrage des Centre for Cybersecurity Belgium (Safeonweb, 12/2024) zeigt, dass 44 % der Belgier Nachrichten an suspekt@safeonweb.be. Im Jahr 2023 waren es 39 %, die E-Mail-Adresse bleibt also attraktiv. Für uns ist dies eine besondere Informationsquelle, die wir in erster Linie für unseren Phishing-Schutzschild (BAPS-System) nutzen, aber auch um die Bürger zu warnen.

Dank all dieser Nachrichten können wir auf Safeonweb.be, Facebook, Instagram und X gezielte Warnungen vor kursierenden Phishing-Nachrichten veröffentlichen. Wir verschicken diese "Warnungen" auch über die Safeonweb-App. Im Jahr 2024 haben wir 81 Warnungen zu den häufigsten aktuellen Phishing-Nachrichten veröffentlicht.

Phishing? Das ist nichts Neues unter der Sonne. Oder etwa doch?

Phishing wird auch im Jahr 2024 eine der am häufigsten genutzten und sich weiterentwickelnden Angriffsmethoden der Cyberkriminalität sein. (Siehe ENISA Threat Landscape, 2024

Auf den ersten Blick sind die meisten Phishing-Nachrichten denen der letzten Jahre sehr ähnlich. Es gibt Nachrichten, die von Behörden, der Polizei, Banken, Itsme usw. zu stammen scheinen, sowie Angebote aus der Kategorie "zu schön, um wahr zu sein", von unwahrscheinlichen Sonderangeboten bis hin zu einmaligen Schnäppchen, und sogar das "verlorene Erbe" ist wieder aufgetaucht

Die Betrüger verfolgen die aktuellen Ereignisse immer noch sehr genau und nutzen aktuelle Ereignisse, um ihren Phishing-Nachrichten Glaubwürdigkeit zu verleihen. So sehen wir zum Beispiel Jahr für Jahr um das Jahresende herum mehr Nachrichten, die sich auf Weihnachtsangebote oder zuzustellende Pakete beziehen.

Dennoch sehen wir 5 Verschiebungen.

1. Smishing und Vishing sind auf dem Vormarsch

Smishing (Phishing per SMS) und Vishing (Phishing per Telefonanruf) sind auf dem Vormarsch. Cyberkriminelle nutzen dies, um direkt Antwort- und 2FA-Codes zu erhalten. Ein Beispiel. Sie rufen ihr Opfer an und geben sich als jemand von Cardstop aus, der helfen will, weil angeblich eine verdächtige Transaktion auf dem Bankkonto stattgefunden hat. Der Betrüger überzeugt das Opfer, z. B. Antwortcodes weiterzugeben oder Itsme zu öffnen und die Authentifizierung abzuschließen.

2. Mehr Phishing über soziale Medien

Plattformen wie LinkedIn, Facebook, Instagram und WhatsApp werden zunehmend zur Verbreitung von Phishing-Links genutzt. Die Grundsätze sind die gleichen wie beim Phishing per E-Mail oder SMS.

3. Mehr personalisierte Angriffe

Durchgesickerte persönliche Daten aus früheren Datenschutzverletzungen personalisieren Angriffe und erhöhen die Glaubwürdigkeit von Phishing, Smishing und Vishing. Betrüger nutzen diese Daten, um Ihr Vertrauen zu gewinnen. Wenn Sie einen Anruf von einem so genannten Bankmitarbeiter erhalten, der Ihren Namen, Ihr Geburtsdatum und andere Details kennt, sind Sie geneigt zu glauben, dass es sich wirklich um einen Bankmitarbeiter handelt.

4. KI und Deepfake-Technologie machen Phishing glaubwürdiger

Cyberkriminelle setzen zweifellos immer häufiger KI ein, um Phishing-Nachrichten zu personalisieren und überzeugender zu machen. Deepfake-Audio und -Video können eingesetzt werden, um CEO-Betrug und Spearphishing zu verfeinern, indem sie die Stimme des CEO eines Unternehmens imitieren. Obwohl solche Praktiken derzeit sicherlich möglich sind, haben wir noch keine konkreten Beispiele entdeckt.

5. Https ist keine Garantie für Sicherheit

Jahr für Jahr stellen wir fest, dass immer mehr Kriminelle SSL-Zertifikate verwenden, um ihre Phishing-URLs vertrauenswürdiger erscheinen zu lassen. Konkret bedeutet dies, dass Sie als Internetnutzer nicht mehr davon ausgehen können, dass eine URL, die mit https beginnt, per Definition sicher ist.

Belgian Anti-Phishing Shield (BAPS)

Dieser Phishing-Schutzschild schützt die Bürgerinnen und Bürger unseres Landes vor Cyber-Kriminellen. Er ist das Aushängeschild des Centre for Cybersecurity Belgium (CCB). Mit dieser Spitzentechnologie gehören wir als kleines Land zur absoluten Weltspitze.

Wie funktioniert das?

1. Das Centre for Cybersecurity Belgium (CCB) erhält Informationen über potenziell bösartige Websites, wenn Internetnutzer verdächtige Nachrichten an verdacht@safeonweb.be weiterleiten.

2. Anhänge und andere Links werden dann aus den verdächtigen Nachrichten extrahiert. Die URLs werden auch aus Screenshots und QR-Codes extrahiert.

3. Es analysiert die URL/den Link/das Attachment. Stellt sich heraus, dass es sich um eine bösartige Website handelt, wird sie aufgelistet und an unsere Partner (ISPs, Google Safe Browsing und Microsoft

SmartScreen) weitergeleitet.

4. Wenn ein Internetnutzer auf einen Link klickt, der zu einer bösartigen Website führt, vergleicht der betreffende Internetdienstanbieter die DNS-Anfrage mit der Liste der bösartigen Websites.

5. Der Benutzer wird dann auf eine Warnseite umgeleitet und kann die bösartige Website nicht besuchen.

Zentrum für Cybersecurity Belgien
Rue de la Loi 18
1000 Brüssel
Belgien
http://www.ccb.belgium.be

Katrien Eggers
Sprecherin(NL/FR/E)
+32 485 76 53 36
katrien.eggers@ccb.belgium.be

Michele Rignanese
Sprecher(NL/FR/E)
+32 (0)477 38 87 50
michele.rignanese@ccb.belgium.be