03 jul 2020 -09:53

Centrum voor Cybersecurity België waarschuwt bedrijven voor factuurfraude

Factuurfraude bij bedrijven is geen nieuw fenomeen maar recent krijgt CERT.be, de operationele dienst van het Centrum voor Cybersecurity België (CCB), meer meldingen van deze manier van oplichting. Het CCB waarschuwt bedrijven dan ook om alert te zijn bij het uitvoeren van betalingen.

Factuurfraude is een vorm van oplichting waarbij cybercriminelen het rekeningnummer laten wijzigen van vaste leveranciers. De cybercriminelen nemen de identiteit aan van een leverancier en vragen een medewerker van de financiële dienst of boekhouding om het rekeningnummer te veranderen en om betalingen uit te voeren. De kans bestaat dat de medewerker niet merkt dat de vraag niet van de leverancier komt en deze betalingen effectief uitvoert naar de rekening van de criminelen.

> "Het ziet ernaar uit dat cybercriminelen tijdens de vakantieperiode steeds vaker hun slag proberen te slaan. Ze rekenen op een verminderde waakzaamheid van de medewerkers tijdens de zomermaanden of hopen dat een vervanger minder goed op de hoogte is van de geldende procedures."
>
> Miguel De Bruycker
> Directeur Centrum voor Cybersecurity België

Een valse factuur heeft verschillende vormen. Cybercriminelen vervalsen originele facturen waarbij ze het bankrekeningnummer veranderen, of sturen spookfacturen, dit zijn facturen waar geen prestatie tegenover staat.

Belangrijkste tips om je te wapenen tegen factuurfraude

Voor management:

- Neem contact op met de aanvrager via een ander telefoonnummer of e-mail dan dat verstrekt is in het ontvangen bericht (om er zeker van te zijn dat dit de echte aanvrager is). Gebruik bv. *forward*, i.p.v. *reply*.
- Zorg ervoor dat de betalingsprocessen duidelijk zijn en goed gevolgd worden.
- Zorg voor duidelijke procedures om betalingsoverdrachten of gevoelige informatieverzoeken te verifiëren, vooral deze via e-mail.

- Informeer medewerkers en zorg dat ze een goede training hebben zodat ze de oplichting snel herkennen en adequaat reageren.

Voor medewerkers:

- Neem contact op met de aanvrager via een ander telefoonnummer of e-mail dan dat verstrekt is in het ontvangen bericht (om er zeker van te zijn dat dit de echte aanvrager is). Gebruik bv. *forward*, i.p.v. *reply*.
- Vergelijk het rekeningnummer op de factuur met je eigen gegevens;
- Wees oplettend op zogenaamde urgente betalingen waardoor afgeweken moet worden van normale procedures.
- Pas beveiligings- en betalingsregels strikt toe. Bijvoorbeeld: betalingen vanaf een bepaald bedrag door meerdere medewerkers laten ondertekenen.
- Beschrijf nooit aan onbekenden hoe betalingen in uw onderneming gebeuren. Hou deze procedures voor intern gebruik.

Zakelijke identiteitsfraude

Bij zakelijke identiteitsfraude handelen cybercriminelen uit naam van je bedrijf. Dit kan plaatsvinden na hacking of door een overname van een bedrijfsaccount. Cybercriminelen kunnen hierdoor bijvoorbeeld met factuurfraude geld stelen van je klanten.

Aanbevelingen om zakelijke identiteitsfraude te voorkomen

- Gebruik altijd sterke wachtwoorden voor je accounts
- Gebruik verificatie in 2 stappen (2FA) waar mogelijk
- Train je medewerkers op het herkennen van phishing
- Ga zorgvuldig om met bedrijfsgegevens

Centrum voor Cyber Security België
Wetstraat 16
1000 Brussel
België
http://www.ccb.belgium.be

Andries Bomans
Communicatieverantwoordelijke
+32 471 66 00 06
andries.bomans@ccb.belgium.be

Katrien - momenteel in verlof Eggers - momenteel in verlof
Communicatieverantwoordelijke
+32 485 76 53 36
katrien.eggers@cert.be