VEILIGHEID IN TIJDEN VAN CRISIS

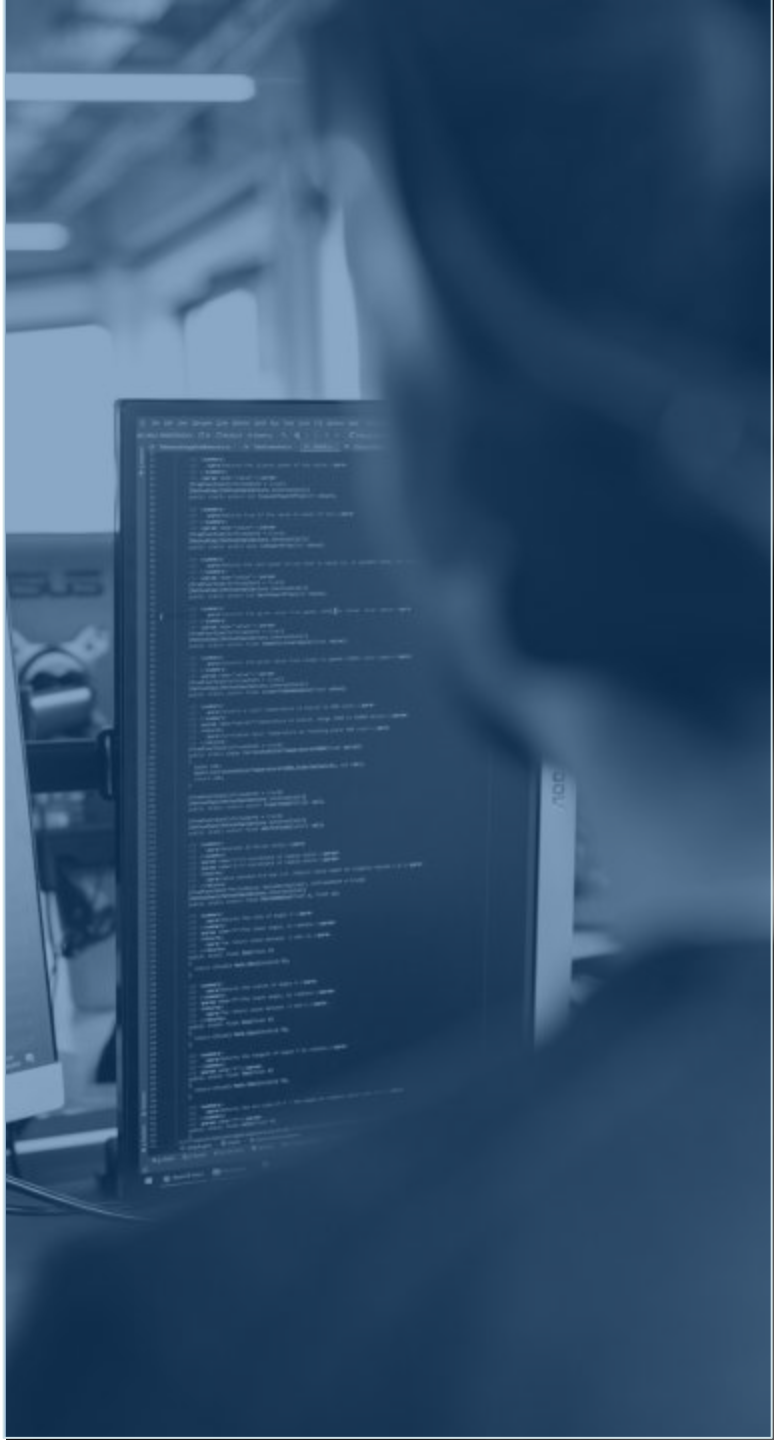
March, 2022

Powered by CYBEREADY

Waarom het belangrijk is

De cyberactiviteit rond het Rusland-Oekraïneconflict laait op en hoewel wij er niet direct bij betrokken zijn, worden ook wij erdoor beïnvloed.

Elke wereldcrisis heeft een cyberdimensie en een scherpe stijging van kwaadwillige phishingmails toont dat deze crisis geen uitzondering op de regel is.



Wat er aan de hand is

1. Beide kampen hebben cyberaanvallen uitgevoerd, met malware die gegevens wist en websites die offline worden gehaald om hun legitieme gebruik te verhinderen.

2. De aanvallen zijn niet altijd doelgericht en besmetten vaak toestellen en websites die niet bij het conflict betrokken zijn. Dat geldt ook voor informatica van uw bedrijf of persoonlijke toestellen.

3. Ook uw persoonlijke accounts op de sociale media kunnen worden gehackt om valse informatie of malware te verspreiden.

Wat u kunt doen om uw thuisnetwerk te beschermen

Installeer de updates van het besturingssysteem en de beveiliging. Als ze beschikbaar zijn, zou u een melding op uw computer of telefoon moeten zien.

Voeg een tweede authenticatiestap toe aan uw accounts op de sociale media (Facebook, LinkdIn, Twitter enz.) en aan uw e-mailaccounts. Neem indien mogelijk ook een back-upaccount voor uw e-mail.

Vertel uw vrienden en familieleden wat er aan de hand is en spoor hen aan om zich ook te beveiligen

Wat u kunt doen om ons netwerk te beschermen

Wij zorgen voor de interne netwerkbeveiliging, zodat u niets technisch' hoeft te doen.

Maar u zou wel meer phishingaanvallen kunnen krijgen. Wees op uw hoede voor e-mails die uw hulp bij technische of financiële zaken vragen.

Controleer altijd het e-mailadres van de afzender – onthoud dat dit de meest cruciale stap is om phishing te detecteren.