Qweb

A TECHONE COMPANY

HOSTING - NIEUWS

AWARENESS

Een gewaarschuwd mens telt voor twee!

1 FEBRUARI

TOENAME CYBERCRIMINALITEIT

PHISHING SIM

info@qweb.nl - 088 208 8088 - qweb.nl

EEN GEWAARSCHUWD MENS TELT VOOR TWEE!

ANNO 2023 KUNNEN BEGRIPPEN ALS CYBERSECURITY NIET MEER ONTBREKEN IN DE BEDRIJFSVOERING.

Onder het motto 'voorkomen is beter dan genezen' is het dan ook van belang om niet alleen je ICT-zaken op orde te hebben, maar ook om je personeel te informeren over hoe zij zichzelf kunnen beschermen tegen cybercriminaliteit.

Als ICT-bedrijf kennen wij als geen ander de kracht van het internet en wat voor voordelen het met zich meebrengt. Als geen ander weten wij echter ook wat de andere kant van de medaille is en dat het internet ook ingezet kan worden voor andere doeleinden.

Door onze eigen ICT-expertise in te zetten willen we dan ook de krachten bundelen met ondernemers om digitale dreigingen in te dammen.

Want wie kan zich beter wapenen tegen cybercriminelen dan ICT'ers zelf?

TOENAME CYBERCRIMINALITEIT

De Covid-19 pandemie heeft ingrijpende veranderingen teweeggebracht voor iedereen. Voor sommigen zijn deze gevolgen nog steeds voelbaar, zo ook in het bedrijfsleven. Eén van de meest alarmerende veranderingen is een explosieve toename van cybercriminaliteit in 2022. Volgens een recent artikel van de NOS (18 januari 2023) blijkt dat cybercriminaliteit in 2022 is verdrievoudigd ten opzichte van voor de coronapandemie, dit is een stijging van 300%. Als we naar de statistieken kijken wordt gesteld dat in 2022 71% van organisaties wereldwijd het slachtoffer zijn geworden van ransomware-aanvallen - en dan hebben we het nog niet gehad over andere soorten cybercrime. Mede hierom is het nu belangrijker dan ooit dat je proactief stappen onderneemt om je beveiligingssystemen tegen digitale dreigingen aan te scherpen.

PHISHING SIM

Phishing is een veelvoorkomende en gevaarlijke vorm van cybercriminaliteit waarbij kwaadwillenden middelen gebruiken om bedrijfsgegevens te stelen. Het duurt slechts enkele minuten voor cybercriminelen je netwerk binnendringen, dus het is belangrijk dat organisaties goed op de hoogte zijn van deze technieken. Phishing-aanvallers proberen gegevens te verzamelen door maatregelen als het verzenden van links naar schadelijke websites, phishing-e-mails die lijken op legitieme communicatie of digitale gijzelingssoftware die gevoelige gegevens verspreidt.

Phishing sim is een educatieve tool die bedrijven helpt bij het trainen van hun medewerkers om kwaadwillende phishing-aanvallen op te sporen. Het simuleert een realistische, maar gerichte phishing-campagne die specifiek is ontworpen voor de aard van de organisatie. Gebruikers kunnen verschillende rollenspellen instellen voor hun medewerkers, inclusief verzenden van phishing-e-mails, oplichters die op zoek zijn naar bankgegevens en digitale gijzeling waarbij kwaadaardige software wordt geïnstalleerd. Gebruikers kunnen ook verschillende scenario's maken om de oefening realistischer en uitdagender te maken. Het voordeel van Phishing Sim is dat het je bedrijf kan helpen om je medewerkers bewust te maken van cybercriminaliteit.

Door tijdens het leerproces feedback te geven aan deelnemers over de manier waarop ze reageren op phishing, kan het hen helpen beter voorbereid te zijn op toekomstige aanvallen.

PRODUCT VAN DE MAAND

DAGELIJKS BACK-UP

Met de dagelijkse back-up van **Veeam** zorgen wij voor een dagelijkse back-up van jouw website/server. Is jouw website gehackt en/of zijn jouw gegevens verloren gegaan waardoorjij een back-up nodig hebt?

Geen probleem, wij hebben direct een recente back-up beschikbaar. Neem voor meer informatie over dit product contact op met onze helpdesk.

QWEB NIEUWS

Afgelopen week hebben wij afscheid genomen van twee stagiaires, namelijk Levi en Leyander. Het kan zomaar eens zijn dat jij één van deze toppers aan de telefoon hebt gehad.

Niet getreurd, want deze week zijn er drie nieuwe stagiairs gestart.

Neem voor vragen gerust contact op met de helpdesk en wie weet krijg jij één van hen aan de telefoon.

Qweb

info@qweb.nl - 088 208 8088 - qweb.nl