cyber Criminaliteit

Cybercriminaliteit is én blijft een hot topic. Internetcriminelen worden alleen maar slimmer en hun methodes veranderen steeds sneller. Het doelwit? Jouw medewerkers. Via hen willen ze binnendringen in jouw bedrijfssystemen en -gegevens. Daarom is het ontzettend belangrijk dat medewerkers de gevaren kennen en veilig werken.

Hoe? Gewoon met betaalbare, slimme beveiligingsoplossingen.

Voorkom dat

- Medewerkers slachtoffer worden van cybercriminaliteit
- Bedrijfsgegevens in de verkeerde handen terecht-komen of kwijtraken
- Cybercriminelen een grote geldsom eisen in ruil voor het ontsleutelen van data
- Bedrijfsprocessen stil komen te liggen
- Jouw bedrijf ernstige imagoschade oploopt

accent

gewoon veilige ICT.

Wapen jouw
organisatie in

3 slimme stappen

Phishingcampagne

Hoe alert zijn jouw medewerkers op cyberaanvallen? Dát testen we met een phishingcampagne. We versturen bijvoorbeeld jaarlijks een neppe mail (phishingmail), waarmee we inspelen op actualiteiten. Net echt.

3 opties

- Phishingmail met *een onbetrouwbare url*, waar jouw medewerker gevraagd wordt om een gebruiksnaam en wachtwoord in te vullen.
- Phishingmail met *een onbetrouwbare bijlage* waarmee cybercriminelen toegang krijgen tot jouw bedrijfsdata als een medewerker deze opent.
- Phishingmail met *een onbetrouwbare koppeling* naar een bijlage op een bekende website, zoals SharePoint of Dropbox.

Natuurlijk heeft de campagne geen échte nadelige gevolgen. We meten alleen hoeveel medewerkers op een link klikken, de bijlage openen of accountgegevens achterlaten. En de resultaten delen we met jou!

Bewustwording

Grote kans dat het aantal medewerkers dat slachtoffer werd van onze phishingcampagne schrikbarend is. Tijd om de resultaten anoniem te bespreken! Dit doen we tijdens een uitgebreide bewustwordingstraining, online of op locatie.

Hierin bespreken we ook de belangrijkste IT-risico's, mogelijke gevaren van de interne werkwijze en handige praktijkvoorbeelden. Daarnaast vertellen we hoe belangrijk het is om op tijd aan de bel te trekken bij twijfel over een bepaalde handeling.

E-learnings

Met één bewustwordingstraining alleen red je het waarschijnlijk niet. Jouw medewerkers moeten continu alert zijn op risico's. Daarom kun je ook gebruikmaken van een digitaal platform met e-learnings. Dit zijn korte trainingen over onder meer IT-risico's en privacy, geactualiseerd op basis van moderne technieken en veelvoorkomende cyberaanvallen.

Het is de bedoeling dat jouw medewerkers de e-learnings binnen een bepaalde tijd doorlopen. Bijvoorbeeld verspreid over een jaar, zodat zij continu alert blijven. Tussendoor sturen wij je uiteraard een voortgangsrapportage.

088 – 30 40 500 verkoop@accent.nl www.accent.nl