DIGITALE OPSPORING

onderdeel van com-connect groep

Presentatie Cybercrime: **Ondernemers Vakdagen Venray (05-10-2016)**
Spreker: **Paul de Vlieger**

Google:
Een zeer bekende en wereldwijd meest gebruikte zoekmachine. Google ondersteunt naast de normale zoekactie ook geavanceerde zoekacties. Zoeken in/naar openbare broncode, video, blogs, discussiegroepen, boeken en news. Daarnaast is er ook een geografische mogelijkheid (maps), een vertaalpagina en de mogelijkheid om alerts in te stellen.

➔ www.google.nl

Google Alerts :
Hier kunt u alarmmeldingen instellen voor naam, creditcard, bedrijf enz. Hiermee wordt u 24/7 op de hoogte gehouden als uw ingestelde (tref)woorden nieuw op het internet worden gevonden. Vergeet niet de zoekopdracht tussen “” te zetten.

➔ https://www.google.com/alerts

Waybackmachine:
Met de Waybackmachine kunt u bekijken hoe websites er in het verleden uit zagen. Dit kan handig zijn wanneer u bijvoorbeeld op zoek bent naar contact gegevens.

➔ http://archive.org/web/

Threat-cloud map:
Via de onderstaande link worden cybercrime aanvallen in kaart gebracht die op dat moment plaats vinden.

➔ https://www.threat-cloud.com/ThreatPortal/#/map

Heeft u al nagedacht over:

1. Internet en data protocol;
2. Training medewerkers;
3. Digitale bewustwording op werkvloer;
4. Digitale bewustwording bij directie;
5. Reguliere externe audits.

Algemene tips voor uw online veiligheid

- ✓ Installeer en update altijd uw internet beveiligingssoftware.
- ✓ Wordt u in een e-mail verzocht op een link te klikken:
  1a. Houdt uw muis stil op de link. Het adres waar de link naartoe leidt wordt nu zichtbaar.
  of
  1b. Open uw webbrowser, typ de link handmatig in.
  2. Controleer certificaat van de website.
- ✓ Verwacht u geen bijlage in een e-mail of eindigt de bestandsnaam van de bijlage op een dubbele extensie (zoals bijvoorbeeld .pdf.zip), klik er dan niet op.
- ✓ Ben altijd voorzichtig met het openen van .zip bestanden. Het zgn. cryptolocker virus schuilt vaak in dit soort bestanden.
- ✓ Bevat een ontvangen e-mail veel grammaticale fouten, ben dan op uw hoede voor phishing.
- ✓ Installeer te allen tijde de updates voor uw besturingssysteem en vermijd het gebruik van illegale software.
- ✓ Goede “gratis” virusscanners zijn zeer schaars.
- ✓ Ben voorzichtig met en op openbare/publieke WiFi-netwerken.
- ✓ Verifieer met wie u online communiceert.
- ✓ Bij gebruik van Facebook (of andere social media sites): Let op uw privacy instellingen!
- ✓ Bij online telebankieren: Vergewis u ervan dat er in de adresregel binnen uw internet browser altijd https://……. staat. Staat dit er niet, log dan niet in. Op de website www.veiligbankieren.nl kunt u meer tips vinden m.b.t. veilig internet bankieren.
- ✓ Test uw eigen kennis op het gebied van cybercrime op www.alertonline.nl

Bedankt voor uw aandacht en interesse in onze organisatie.

Indien u vragen heeft of nadere info wenst, kunt u te allen tijde contact met ons opnemen

Bedrijfsinformatie

Digitale Opsporing BV

Digitale Opsporing BV is een door het ministerie van Veiligheid en Justitie erkend particulier digitaal forensisch recherchebureau en cyber security specialist, werkzaam onder nummer POB 1182.

Digitale Opsporing BV levert een breed scala aan diensten. Onze medewerkers zijn gespecialiseerd in het verrichten van particulier (fraude) onderzoek, internet recherche onderzoek en digitaal forensisch onderzoek. Daarnaast bieden wij een training Internet Rechercheren aan op diverse niveaus. Voor instanties die gebruik maken van het IRN netwerk bieden wij IRN trainingen aan. Ons team bestaat uit gecertificeerde forensische professionals en (digitale) rechercheurs afkomstig van politie Nederland.

Contactgegevens:
Digitale Opsporing BV
Spoorstraat 5
5975 RK Sevenum
085-489 12 50
www.DigitaleOpsporing.nl
Loket@digitaleopsporing.nl