

m uw kroonjuwelen ionage

dig steeds beter dat digitale veiligheid een randvoorwaarde
e veiligheid een integraal onderdeel te laten zijn van
Danny Pronk, Principal Intelligence Consultant, minder
er innoveren en zo geld besparen.



Danny Pronk,
Principal Intelligence Consultant

enwoordig is veel
ge digitaal geworden:
urrenten hacken bijvoor-
bedrijfscomputers om
levolle informatie te
Maar ook op de klas-
manier wordt veelvuldig
ionage gedaan, bijvoor-
door medewerkers te
eren en hen te gebruiken
egang te krijgen tot
aters, de bedrijfslocatie
ormatie. Spionnen vallen
nderneming op verschil-
manieren aan. Elke

poort, of het nu de receptie,
een medewerker, of het
IT-netwerk betreft, is een po-
tentiële ingang. En spionnen
zijn altijd op zoek naar deze
ingangen. De kans dat ze zo'n
ingang vinden is ook groot.
Zoek daarom een goede ba-
lans in wat er online gedeeld
wordt. Post niet op LinkedIn
of Facebook dat er waardevolle
informatie te halen is.
Bescherm alle apparaten.
Spionnen zijn geïnteresseerd
in alle informatie op tele-

foons, tablets en laptops. Wees
ook alert op phishing-mails,
installeer beveiligingssoftware
en zorg dat deze up-to-date
zijn. Ondernemers moeten
het idee omarmen dat digitale
veiligheid niet langer een
IT-probleem is, maar een
randvoorwaarde voor duur-
zaam en toekomstbestendig
zakendoen. Om als onderne-
ming in business te blijven en
te groeien, is digitale veilig-
heid een absolute voorwaar-
de. Het is belangrijk voor het
behouden van klanten en
moet een integraal onderdeel
zijn van de bedrijfsvoering.

Het is als ondernemer ook
belangrijk te beseffen hoeveel
risico's worden gelopen, en
bijpassende dreigingsscenario's
te maken. Door digitale
veiligheid te bekijken met
een zakelijke bril, en dit te
koppelen aan elke zakelijke
beslissing die genomen wordt,
kunnen spionagerisico's
worden verkleind, en kan
sneller worden geïnnoveerd
en geld bespaard."

Endpoint Protection



Emil Pilecki,
Security Specialist

Bij Rootsec werd al langer veel aandacht
besteed aan Endpoint Protection en dat
blijft toenemen. Endpoints zijn - de naam
zegt het al - de eindpunten die verbonden
zijn en informatie uitwisselen met een net-
werk, zoals bijvoorbeeld laptops en desktop
pc's. "Endpoint Protection is eigenlijk het
constant actief monitoren en beveiligen
van endpoints tegen cyberdreigingen zoals
virussen, malware en ransomware", vertelt
CEO Emil Pilecki. "Het is een offensieve
laag van extra beveiliging die aanvallen de-
tecteert, blokkeert of voorkomt. Aangezien
70 procent van de cyberaanvallen begint
bij de eindgebruiker, is dit een uiterst be-
langrijke beveiligingslaag."

De Endpoint Protection-oplossingen
van Rootsec beschikken over flink wat
extra denkkracht, want ze worden voor
een belangrijk deel aangedreven door
AI. Pilecki: "Dat geeft onze software de
capaciteiten om nieuwe soorten bedrei-
gingen te signaleren. De AI ziet bepaalde
patronen en gedrag dat afwijkt van het
gebruikelijke. Dat kan aanleiding geven om
in te grijpen. Zo'n ingreep volgt bijvoor-
beeld direct als een gebruiker op het punt
staat een gevaarlijk bestand te openen of
als kwaadwillenden in de systemen zijn ge-
komen. Daarmee zijn we zeer succesvol en
voorkomen we ontzettend veel ellende. We
blijven non-stop bezig om onze oplossin-
gen nóg beter te maken, zodat we altijd de
veiligheid kunnen blijven garanderen."

ng Director: Jonathan Andersson Redactie: Jerry Huinder Graphic Design: Liese Oers, Mo Aslan
n, Diederik de Groot, Leendert van der Ent, Gedistribueerd met: Het FD 2023 Drukkerij: RODI Rotatiedruk
in samenwerking met onze klanten. Dit zijn commerciële uitingen. Dit is een commerciële uitgave.
ctie.



Uitgegeven door
Contentway B.V.
Keizersgracht 424
NL-1016 GC Amsterdam

Tel: +31 20 808 82 00
Web: contentway.nl
Email: info@contentway.nl
redactie@contentway.nl

ADVERTENTIE

schap wordt
ligen tegen
een sterke
is deze partner
betaalbare
KB.

TRAIN

DOWNLOAD
DE GAME GRATIS

jezelf en jouw collega's nu op