OfficeGrip

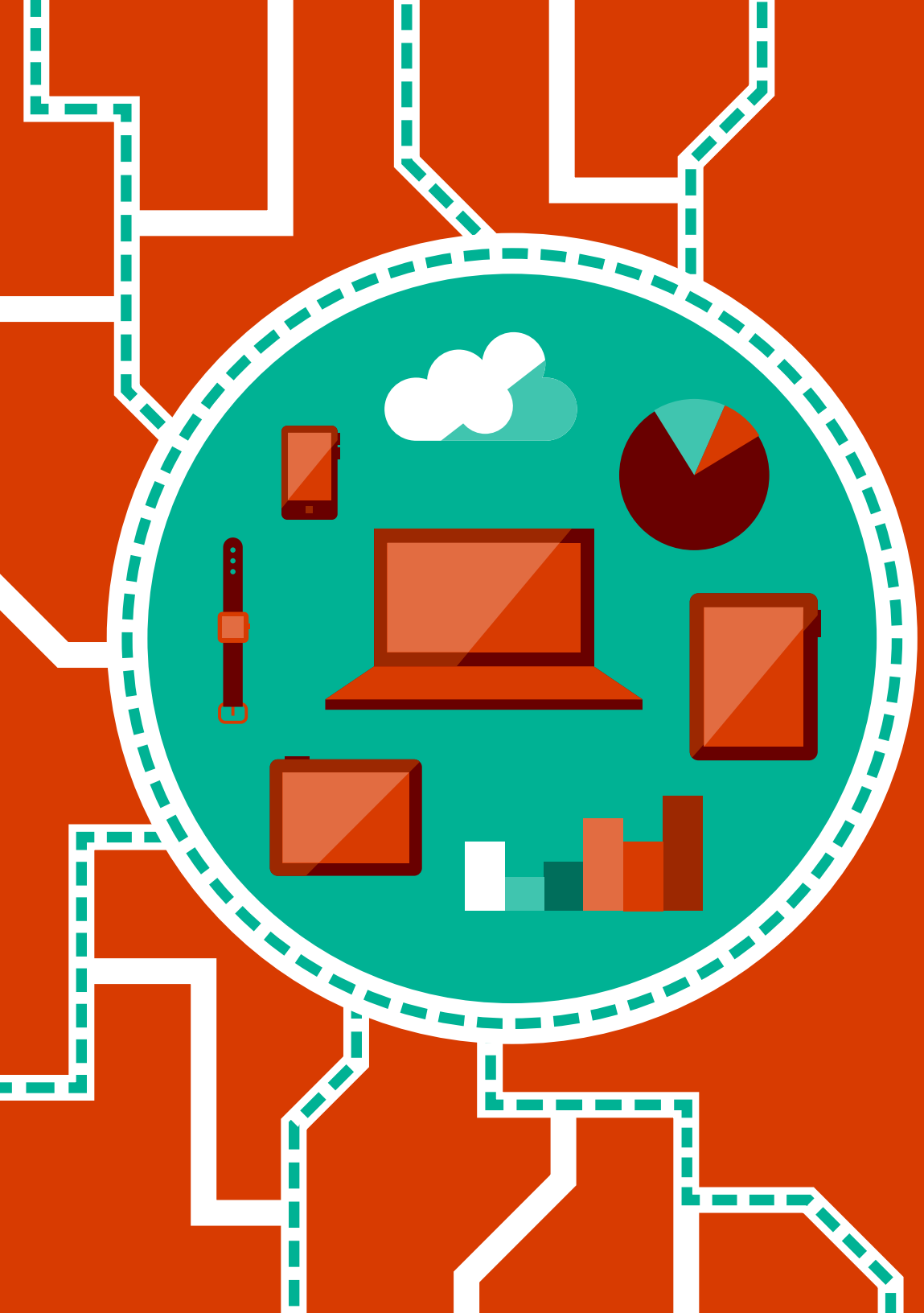
De zeven soorten effectieve hackers

Effectieve benaderingen van cyberbeveiliging

Microsoft

Digitale transformatie beïnvloedt elk aspect van je organisatie; het geeft vorm aan groei, transformeert producten, optimaliseert bedrijfsvoering en geeft werknemers meer mogelijkheden. Deze buitengewone kansen gaan echter gepaard met vele vragen over hoe IT-leiders hun organisaties effectief kunnen ontwikkelen terwijl ze hun gegevens beschermen tegen steeds ernstigere cyberaanvallen.

HET BEDREIGINGSLANDSCHAP. De snel verdwijnende IT-perimeter heeft nieuwe doelwitten gecreëerd voor hackers. En hackers worden steeds bekwamer en georganiseerder. Als gevolg daarvan is het aantal, het raffinement, de ernst en de financiële impact van verschillende aanvalsvectoren over de hele wereld in ongekende mate toegenomen. Bedreigingen variëren nu van onruststokende tieners die in hun eentje op hun laptop zitten te hacken zodat ze erover kunnen opscheppen, tot zeer georganiseerde criminele groepen die de macht hebben om de nationale en internationale veiligheid te bedreigen.



HET GOEDE EN SLECHTE NIEUWS. Laten we beginnen met het slechte nieuws. Voornamelijk vanwege de zeven verschillende soorten hackers die in dit eBook worden beschreven, neemt cybercriminaliteit exponentieel toe. Miljoenen euro's aan intellectueel eigendom lopen risico, en dan is er ook nog eens verloren productiviteit. Het goede nieuws is dat je organisatie er niet alleen voor staat in de bestrijding van deze criminelen. Hoewel de realiteit duidelijk afschrikwekkend is, verkeert Microsoft dankzij zijn enorme omvang en wereldwijde bereik in een unieke positie om je te helpen er iets aan te doen.

Vanwege de enorme hoeveelheid informatie die Microsoft verwerkt – zoals miljarden apparaatupdates en miljarden e-mails en verificaties – kunnen wij bedreigingsgegevens veel sneller synthetiseren dan jouw organisatie ooit alleen zou kunnen doen. – Microsoft-blog "Microsoft's unique perspective on cybersecurity." 24 juni 2016. *[Ons] unieke inzicht in het bedreigingslandschap, verkregen via biljoenen signalen uit miljarden bronnen, creëert een intelligente beveiligingsgrafiek aan de hand waarvan we bepalen hoe we alle eindpunten beveiligen, aanvallen beter detecteren en sneller reageren.* – Bret Arsenault, Chief Information Security Officer bij Microsoft, 2015 – Microsoft-blog "Enterprise security for our mobile-first, cloud-first world." 17 november 2015.

De statistieken van cybercriminaliteit zijn ontstellend

Voor 2015 werden er alleen al in de Verenigde Staten **2.400** klachten over **RANSOMWARE** ingediend bij het Internet Crime Complaint Center – en dat kostte **$24 MILJOEN**

(FBI-persbericht, 2016)[1]

Hoe vaak is er een nieuw slachtoffer van identiteitsfraude? Elke 2 SECONDEN

(Javelin, 2015)[2]

Volgens het National Crime Agency (NCA) **OVERTROF CYBERCRIMINALITEIT** in 2016 alle andere vormen van criminaliteit in het Verenigd Koninkrijk

(Dark Reading, juni 2016)[3]

Toename met **600%** van **bijlagegebaseerde** vs. **via URL's bezorgde malware-aanvallen** van half 2014 tot 2015

(Proofpoint, 2015)[4]

IN 2015 werden 594 MILJOEN mensen over de hele wereld het slachtoffer van **ONLINE CRIMINALITEIT**

(2016 Norton Cybersecurity Insights Report)[5]

$209 MILJOEN gestolen in het eerste kwartaal van 2016 via **CYBERBEDREIGINGEN** en **RANSOMWARE**

(FBI-rapport, april 2016)[6]