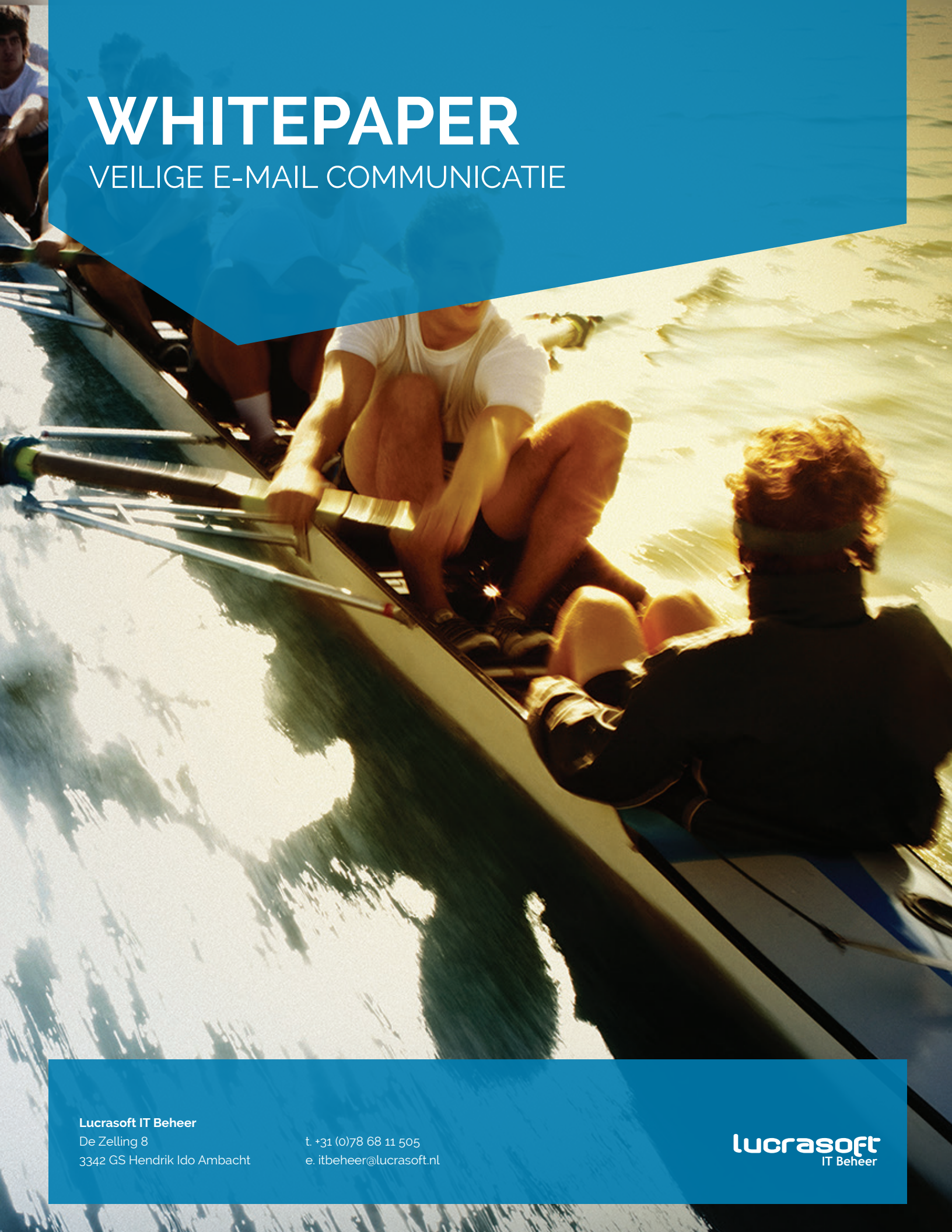
WHITEPAPER

VEILIGE E-MAIL COMMUNICATIE



Lucrasoft IT Beheer
De Zelling 8
3342 GS Hendrik Ido Ambacht

t. +31 (0)78 68 11 505
e. itbeheer@lucrasoft.nl

lucrasoft
IT Beheer

E-mail: 50% is ongewenst

Ruim de helft van al het e-mailverkeer bestaat uit ongewenste e-mail, ofwel spam. Dit heeft ten doel de ontvanger te verleiden iets te kopen, op te lichten, zijn computer te gebruiken voor cyberaanvallen of om deze te besmetten. Dit wordt gedaan d.m.v. malware, een vorm van criminaliteit die zowel massaal als innovatief is, elke dag worden duizenden nieuwe vormen van malware (kwaadaardige software) ontdekt. In deze whitepaper lichten we het gevaar van cryptolockers, een op dit moment veel gebruikte vorm van malware, nader toe en beschrijven we een nieuwe oplossing van Microsoft.

Wat is een cryptolocker?

Actueel op dit moment zijn de cryptolockers. Deze vorm van malware valt in de categorie ransomware, waarbij data gegijzeld wordt. Wanneer een e-mail met deze malware geopend wordt, zullen je bestanden versleuteld worden. In de meeste gevallen wordt losgeld geëist in de vorm van bitcoins, waarna belooft wordt om de gegijzelde data weer vrij te geven. Garantie dat dit daadwerkelijk gebeurt, is er echter niet.

Het is een applicatie

Gemaakt om bestanden te versleutelen

Doel: geld verdienen

"Steeds meer bedrijven en particulieren krijgen al te maken met cybercriminelen. Één op de vijf bedrijven heeft te maken met de gevolgen van cyberaanvallen en dit zal de komende jaren alleen maar toenemen."

Lucrasoft IT Beheer
De Zelling 8
3342 GS Hendrik Ido Ambacht

t. +31 (0)78 68 11 505
e. itbeheer@lucrasoft.nl

lucrasoft IT Beheer

Bescherm je organisatie

Het risico op besmetting bij een cyberaanval is nooit tot 0% te reduceren, maar door de juiste voorbereidingen te treffen kan het wel ingeperkt worden. Het grootste gevaar en tevens de reden dat het risico nooit volledig is af te dekken is een menselijke fout. Daarom is bewustwording creëren bij het personeel veruit de belangrijkste voorzorgmaatregel die genomen moet worden. Maak mensen bewust dat ze voorzichtig moeten met het openen van e-mails van onbekende afzenders. Open geen bijlagen, klik niet op links van onbekenden of berichten die er verdacht uit zien. Weet je niet goed hoe je je mensen traint, neem dan contact met ons op voor een training door onze ervaren IT engineers.

Neem technische maatregelen

Zorg tevens voor de juiste technische maatregelen zoals goede spamfilters, een virusscanner en firewall. Voorkom gevaren door verouderde software versies en update regelmatig. In veel updates worden issues opgelost, zogenaamde gaten, waar cybercriminelen gebruik van maken. Ten slotte is je back-up een laatste redmiddel. Mocht het onverhoopt toch mis gaan, kan eventuele schade beperkt blijven door het terughalen van een back-up.

1. Bewustwording van personeel

2. Spamfilters (EOP en ATP)

3. Virusscanner (Webroot)

4. Updates

5. Back-up

Onze partners

Microsoft Partner
Gold Small and Midmarket Cloud Solutions
Microsoft

WEBROOT
SecureAnywhere®

Lucrasoft IT Beheer
De Zelling 8
3342 GS Hendrik Ido Ambacht

t. +31 (0)78 68 11 505
e. itbeheer@lucrasoft.nl

lucrasoft
IT Beheer

Filter berichten, leg een extra veiligheidslaag aan

In deze whitepaper gaan we extra in op de nieuwe mogelijkheden die Microsoft biedt met Exchange Online Protection (EOP). Dit is een e-mailfilterservice in de cloud die je helpt je organisatie te beschermen tegen spam en malware. Elk bericht moet het EOP filter passeren en vangt e-mails af waarvan vermoedt wordt dat ze een verhoogd risico vormen.

Hoe werkt Exchange Online Protection?

- **1. Een bericht komt binnen en gaat door het filter**
- **2. De filter controleert de reputatie van de afzender en inspecteert het bericht op malware**
- **3. Berichten worden gefilterd op basis van transportregels**
- **4. Berichten worden gefilterd op inhoud, waarbij de inhoud wordt gecontroleerd op berichtkenmerken die specifiek zijn voor spam.**
- **5. Zodra het bericht al deze beveiligingslagen succesvol heeft doorlopen, wordt het bericht bezorgd aan de ontvanger.**

Extra hulp voor je medewerkers

Verbindingsfilter

Het is mogelijk zelf een lijst te maken met IP-adressen van veilige afzenders of IP-adressen waarvan de berichten geblokkeerd moeten worden.

Transportregels

De transportregels kan je zelf opstellen op basis van je bedrijfsbeleid. Je kan bijvoorbeeld een regel opstellen die ervoor zorgt dat een notificatie wordt gestuurd naar een manager wanneer er een bericht binnenkomt van een specifieke afzender.

Berichtkenmerken

Je kan zelf instellen of berichten in bepaalde talen of uit bepaalde landen of regio's als spam aangemerkt moeten worden.

Lucrasoft IT Beheer
De Zelling 8
3342 GS Hendrik Ido Ambacht

t. +31 (0)78 68 11 505
e. itbeheer@lucrasoft.nl

lucrasoft IT Beheer

Veiligheid en betrouwbaarheid vanuit de cloud

Microsoft geeft de garantie dat met EOP 100% van de bekende virussen en 99% spam wordt tegengehouden. Om dit te realiseren wordt gebruik gemaakt van een wereldwijd netwerk van datacenters om ervoor te zorgen dat het netwerk 99,999% van de tijd beschikbaar is. Als een datacenter onbereikbaar is, worden e-mailberichten automatisch naar een ander datacenter gestuurd, zonder dat de service wordt onderbroken. Berichten worden namens jou geaccepteerd door de datacenters, zodat de last voor je eigen servers wordt verkleind. Daarnaast wordt continue gewerkt om met de nieuwste technieken je e-mailomgevingen nog beter te beveiligen.

"Er worden continue nieuwe technieken toegepast om je e-mail nog beter te beveiligen. Daarnaast maak je gebruik van de e-mailbeveiliging van het gerenommeerde bedrijf Microsoft. "

Verschillende vormen van EOP

EOP kan je e-mailomgeving beveiligen in verschillende scenario's. EOP zorgt standaard voor de beveiliging van de Exchange Online-postvakken in de cloud. Als je gebruik maakt van de postvakken van Microsoft Office 365, worden deze automatisch beveiligd door EOP. Daarnaast kan EOP e-mailbeveiliging in de cloud bieden voor on-premise e-mailoplossingen.

Office 365

Exchange Online

Lucrasoft IT Beheer
De Zelling 8
3342 GS Hendrik Ido Ambacht

t. +31 (0)78 68 11 505
e. itbeheer@lucrasoft.nl

lucrasoft IT Beheer