

GROEP 9 PHILIPS ELECTRONICS

Philips Electronics

Soorten ICT-diensten:

Philips maakt gebruik van een breed scala aan ICT-diensten om hun operaties te ondersteunen. Ze hebben een afdeling genaamd "Innovation Hub Eindhoven" die zich richt op het verbinden van mensen, technologie en processen om waarde te creëren voor klanten. Ze hebben expertise in digitale en systeemarchitectuur, datawetenschap en AI, softwareconcepten, Internet of Things en connectiviteit, sensorisatie, medische beeldvorming en pathologie, klinische en operationele informatica, service- en oplossingsontwerp, gebruikerservaring ontwerp, gedragswetenschappen en minimaal invasieve interventietechnologieën.

Bron: Philips.com

Formaat van bedrijf:

Philips is een groot wereldwijd conglomeraat met een marktwaarde van meer dan 26 miljard Amerikaanse dollars. Het bedrijf heeft activiteiten in meer dan 60 landen. Wat betreft het aantal werknemers, Philips had in 2022 ongeveer 74.451 werknemers.

Bronnen: statista.com & en.wikipedia.org

Afhankelijkheid van derden:

Philips heeft samengewerkt met andere bedrijven om hun doelen te bereiken. Een voorbeeld hiervan is hun joint venture met LG Electronics, waarbij ze hun wereldwijde cathode ray tube ("CRT") bedrijven hebben gecombineerd. Bovendien biedt Philips contractontwerp en -ontwikkeling voor derden van elektronische, optische en mechatronische medische apparaten, componenten daarvan en prototypes.

Bronnen: engineeringolutions.philips.com & ec.europa.eu

Bedrijfs flags

Welk bedrijf verzorgt pakketbezorging?

Wat: Philips verstuurd pakketten naar klanten via UPS en PostNL

Waar: Philips online-store ondersteuning. <https://www.philips.nl/c-w/consumenten-ondersteuning/online-store-faq>

Welke verzendopties en vervoerders zijn beschikbaar?



Houd er rekening mee dat er voor sommige artikelen vanwege de grootte of kwetsbaarheid beperkte verzendopties beschikbaar zijn. Afhankelijk van de beschikbaarheid kunnen de volgende verzendopties worden geselecteerd tijdens de bestelprocedure:

Carrier	Delivery time frame	Price
UPS standard	2-3 business days	€ 5.99
UPS Express	2-1 business days	€ 6.99
UPS Pick up Point	2-1 business days	€ 3.99
PostNL (without tracking)	3-4 business days	€ 0.99
PostNL standard	2-3 business days	€ 5.99
PostNL Access Point	2-3 business days	€ 3.99

Risicoanalyse: Als aanvaller zou ik nu kunnen voordoen als UPS bezorger en klantgegevens vinden door de pakketten aan klanten.

- Oplossing: Deze informatie alleen maar weergeven aan mensen die een Philips Account hebben of een bestelling hebben geplaatst.

Welke e-mail client?

- Wat: Philips.com valt onder Outlook

Waar: <https://mxtoolbox.com/emailhealth/philips.com/>

Mail Server mx.philips.com			
Pref	Hostname	IP Address	TTL
0	philips-com.mail.protection.outlook.com	52.101.68.10	60 min
dmarc.philips.com			
Category	Host	Result	
✓ dmarc	philips.com	DMARC Record found	More Info
✓ dmarc	philips.com	The record is valid	More Info
✓ dmarc	philips.com	All external domains in your DMARC record are giving permission to send them DMARC reports	More Info
✓ dmarc	philips.com	Multiple DMARC records corrected to a single record	More Info
✓ dmarc	philips.com	DMARC Quarantine/Reject policy enabled	More Info
smtp.philips-com.mail.protection.outlook.com			
Category	Host	Result	
⚠ smtp	philips-com.mail.protection.outlook.com	May be an open relay	More Info
✓ smtp	philips-com.mail.protection.outlook.com	OK - 52.101.73.19 resolves to mail-as0pr04cu0003 inbound.protection.outlook.com	More Info
✓ smtp	philips-com.mail.protection.outlook.com	OK - Reverse DNS is a valid Hostname	More Info
✓ smtp	philips-com.mail.protection.outlook.com	OK - Reverse DNS matches SMTP Banner	More Info
✓ smtp	philips-com.mail.protection.outlook.com	OK - Supports TLS	More Info
✓ smtp	philips-com.mail.protection.outlook.com	0.291 seconds - Good on Connection time	More Info
✓ smtp	philips-com.mail.protection.outlook.com	1.039 seconds - Good on Transaction Time	More Info

Risicoanalyse: Er is nu bekend welk protocol wordt gebruikt en Outlook als client. Mocht ik nu binnen willen dringen op iemands Outlook word het erg gemakkelijk.

Oplossing: Een overeenstemming met outlook om dit soort gegevens te verbergen of meerdere domeinen gebruik dan enkel philips.com

Heeft het bedrijf datacentra in eigen beheer, huren ze ruimte in een datacenter, huren ze apparatuur, of gebruiken ze een cloud platform?

Wat: Philips Speechlive = Azure server, Philips Healthcare = AWS, Philips Electronics op High Tech Campus uitbested.

Waar: Google en Google Maps

Datacenter Eindhoven 2. De digitale groeiambities:

Met dit nieuwe datacenter (de High Tech Gateway) ondersteunt NorthC de digitale groeiambities van Eindhoven en Brabant. Multinationals zoals Philips, NXP en Intel, maar ook tal van mkb-ondernemingen, onderzoeksinstituten, servicebedrijven en starters werken hier samen aan innovaties die de wereld gaan veranderen. Al deze hightech activiteit vraagt om een deskundige datacenterpartner die thuis is in de regio, die de juiste partijen bij elkaar brengt en die connectiviteit biedt met belangrijke cloudproviders en carriers binnen de regio én met de grote internetknooppunten rond Rotterdam en Amsterdam.

<https://www.northcdatacenters.com/northc-datacenters/eindhoven-2/>

Risicoanalyse: Wetend waar het datacenter zich bevind kan er makkelijker informatie van het datacenter worden getapt.


- Oplossing: Dit soort gegevens zijn eigenlijk niet te verstoppen, maar het zou verborgen kunnen worden met wie NorthC in partnerschap gaat.







Heeft het bedrijf veel medewerkers die op afstand werken?

Wat: Dat Philips erg flexibel is met buiten het kantoor werken.

Waar: <https://builtin.com/company/philips/benefits>

Culture



 Volunteer in local community	 Flexible work schedule
 Open office floor plan	 Remote work program
 Employee resource groups	 Hybrid work model

Risicoanalyse: Er is bekend dat medewerkers vanuit huis werken, specificeer je tot 1 medewerker, zoek zijn adres en ga inbreken op zijn thuisnetwerk.

Oplossing: Ik had ook een site gevonden wat deze benefits blokkeert. Dit soort dingen verbergen voor mensen die niet werken bij Philips of niet willen werken bij Philips helpt enorm. Meer mensen naar locatie komen waar inbreken op het netwerk onmogelijk wordt.

Persoonlijke flags

Wat zijn het interne telefoonnummer & e-mailadres van de medewerker?

Wat: de interne telefoonnummer & e-mailadres zijn:

Tel: +31 20 59 77055

Mail: leandro.mazzoni@philips.com

Waar: deze informatie is te vinden op de site van Philips zelf

[Philips announces CEO succession - News | Philips](#)



Leandro Mazzoni

Philips Investor Relations

Tel: +31 20 59 77055



Risicoanalyse: het bekend geven van een intern telefoonnummer en/of kan leiden tot ongevraagde communicatie, ook kan het helpen bij het bouwen van een profiel over iemand.

Oplossing: Deze informatie kan verborgen worden, of de gegevens van een secretaris of iets dergelijks.

Hoe lang werkt de werknemer al bij het bedrijf?

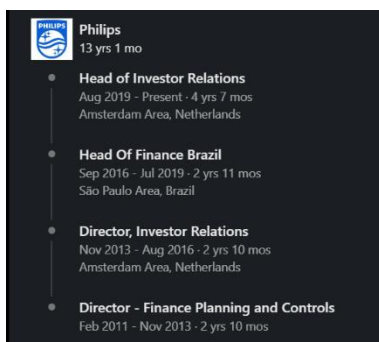
Wat: we hebben gevonden dat Leandro al bijna 14 jaar bij Philips werkt

Waar: Dit stond openbaar op zijn LinkedIn

Risicoanalyse: Het weten van hoelang iemand ergens werkt opzich is niet erg risicovol, echter kan je beter een profiel maken met deze info.

met deze informatie kun je ervan uitgaan dat deze persoon toegang heeft tot veel gevoelige informatie binnen het bedrijf, dit is handig om te weten wanneer je een gerichte aanval wil doen.

Oplossing: Leandro zou zijn werkervaring van LinkedIn kunnen weghalen



[Experience | Leandro Mazzoni | LinkedIn](#)

Heeft de medewerker recentelijk (of binnenkort) belangrijke werkgerelateerde evenementen? Wat:

we hebben gevonden dat Leandro aanwezig was bij een evenement van Black history month op 1 februari, in de New York stock exchange

Waar: deze informatie stond openbaar op LinkedIn.

Risicoanalyse: Aangezien dit een dag na het evenement was geplaatst konden we hem niet

zogenaamd in lijve opzoeken. Maar we kunnen concluderen dat Leandro wel aanwezig is bij andere evenementen.

Oplossing: Geen beelden plaatsen van de medewerkers die aanwezig zijn bij een evenement.



Pretext & Spearphising:

Pretext:

Wie & wie: Ik ben een balie medewerker van de New York Stock Exchange en zoek contact met Leandro Mazzoni.

Waarom: Ik wil hem wijs maken dat hij een voorwerp is verloren op het evenement waar hij aanwezig was rond 1 Februari

Wat: Ik wil graag weten of ik hem mag benaderen op zijn werkmail of liever op zijn privemail

Vraag & Antwoord: telefoongesprek: "Hello Mr. Mazonni, I would like to notify that we likely found a suitcase of yours in the New York Stock Exchange building, I would like to confirm this object is yours, what mail can I contact you on (hier krijgen we zijn werkmail(die we al hebben) of zijn prive-email (dit zouden we liever hebben))."

Context: dit gesprek zou ik proberen telefonisch uit te voeren

Succeskans: Ik acht dat er best een succeskans is, we hebben een directe telefoonlijn naar Leandro en desnoods hebben we nog zijn werkmail die we gevonden hebben op de site van Philips.

Stappen om een spoof mail op te stellen:

- Reconnaissance: Het uitzoeken van het bedrijf, medewerkers om te achterhalen hoe je een slachtoffer van je gekozen bedrijf het best kan benaderen en misleiden via een mailtje.
- Eigen spoof mailadres opzetten via SMTP: Als aanvaller zit je natuurlijk zelf niet in het netwerk van het bedrijf waarvanuit je je mail verstuurt. Je zult dus je eigen mailadres nog moeten opzetten via een mailprotocol op de echte mailserver van het bedrijf. Dit kan door middel van het SMTP protocol.
- Nadat alles duidelijk is over het bedrijf en medewerker; neem emailadres, functie, evenementaanwezigheid is het tijd om een pretext op te stellen en je voor te doen als een werkend

persoon bij (...) bedrijf of locatie.

- De spoof mail moet logisch overkomen en formeel, geen spelfouten en een payload bevatten om het spoofen op de PC van de gekozen medewerker op te kunnen zetten.

Spearphising mail:

From: newyork@sec.gov (spoof)

Dear Mr. Mazzoni,

On February 1st the New York Stock Exchange hosted a Black History month event which you attended with your colleagues from Philips.

During our hosted event it seemed you lost [the following object](#).

After finding the object we kept it stored behind our information desk.

Please verify that this object is yours so we can send it back to you.

With kind regard,

New York Stock Exchange

Geef behalve de e-mail zelf ook aan vanaf welk e-mail adres je dit bericht zou kunnen sturen en waarom je verwacht dat je spearphishingpoging zou kunnen werken. Bedenk ook hoe je een payload zou aanleveren. Waarom die methode? Er wordt gemaaild vanaf newyork@sec.gov en deze spearphishingpoging heeft veel kans van slagen vanwege het feit dat Leonardo Mazonni bij de genoemde event echt is geweest, er wordt niet duidelijk gemaakt wat er kwijt is geraakt wat ook direct de verstopte payload is. Nu ter voorbeeld is het een hyperlink maar er wordt gebruik gemaakt van een png spoof payload. Een png wat dan het "vermiste object" weergeeft maar eigenlijk dus op zijn PC inbreekt.