Is jouw organisatie cybercrime proof?

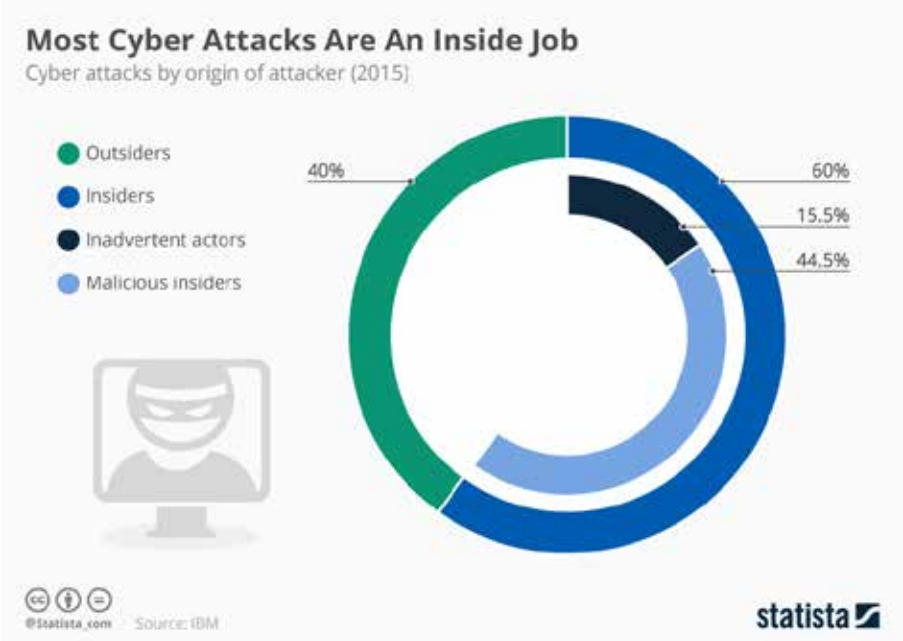
Praktische checklist voor een veilige werkomgeving

“Data 174.000 Nederlanders gelekt bij Uber-hack”
“Malware ingezet om duizenden telefoons te bespioneren”
“Aantal slachtoffers ransomware Wannacry loopt op tot 200.000”

Van bijna elke organisatie zijn gehackte emailadressen en wachtwoorden te vinden op het dark web waarmee cybercriminelen proberen jouw organisatie binnen te komen.
Dit soort headlines verschijnen steeds vaker in het nieuws. De Wannacry aanval van mei 2017 ligt bij veel mensen nog vers in het geheugen. Zoals bij Q Park waar 11 parkeergarages vijf dagen plat lagen. Betaalautomaten werkten niet, slagbomen werden opengezet om mensen toch te kunnen laten wegrijden. De financiële impact van dit soort events is gigantisch, en dan hebben we het nog niet over de reputatieschade.

Cybercriminaliteit ontwikkelt zich in een angstaanjagend snel tempo door technologische mogelijkheden en het rendabeler worden van de aanvallen. De opzet van de aanvallen verandert ook: hackers en criminelen gaan steeds meer met scherp schieten in plaats van met hagel. Gevaarlijker, dat klopt, het grote gevaar schuilt namelijk in de onopvallendheid van deze aanvallen. Een terloops mailtje van je CEO die vraagt of je deze rekening zo snel mogelijk wilt betalen. Je hebt niet in de gaten dat dit niet van je CEO komt, zo echt ziet het er uit. Zoals de NOS[1] kopte: ‘Een goede hack hoeft helemaal niet complex te zijn’. Cyberaanvallen worden inderdaad steeds geraffineerder: het zijn juist de aanvallen die inspelen op het sentiment van de eindgebruiker die zo gevaarlijk zijn.

*Bron: NOS.nl nos.nl/artikel/2213156-een-goede-hack-hoeft-helemaal-niet-slim-te-zijn.html



Bron: IBM en Statista

Met stip op 1: menselijke fout

*Bron: Statista www.statista.com/chart/4994/most-cyber-attacks-are-an-inside-job/

IBM publiceerde al eens dat de meeste datalekken en cyberaanvallen een ‘inside job’ zijn.[2] Uit onderzoek is gebleken dat 60% van de virusbesmettingen worden veroorzaakt door een medewerker. Een menselijke fout dus. Dat komt bijvoorbeeld:

- door het klikken op een verkeerde link (phishing emails),
- het downloaden van apps buiten de officiële kanalen, of
- het openen van besmette bijlagen in een email.

Wat we daarnaast vaak zien, is dat medewerkers het overzicht kwijtraken van waar alles staat. Waar kan ik veilig documenten opslaan? Hoe kan ik thuis verder werken aan die belangrijke offerte?

Het gevolg is dat er chaos ontstaat bij medewerkers en binnen de organisatie. Hoe beveilig je je organisatie als alles overal en nergens staat? Heel simpel: niet. Dat is onmogelijk waterdicht te krijgen.

TIP

Controleer preventief je online omgeving

Laat periodiek een scan uitvoeren die digitale kwetsbaarheden aan het licht brengt en die laat zien welke informatie van jouw organisatie op het dark web te vinden is. Of huur een ethical hacker in, die je laat proberen om in te breken op je online werkomgeving en website.
Deze resultaten kun je gebruiken om een inschatting te maken van de kosten die kunnen oplopen bij een echte hack. Bovendien is het een startpunt om een roadmap te maken om de informatiebeveiliging binnen je organisatie te verbeteren.

Checklist: 5 aandachtspunten voor een veilige werkomgeving

Informatiebeveiliging is een must met geavanceerde cyberaanvallen die op de loer liggen, en met strengere wetgeving, zoals de GDPR. Aan de hand van een praktische checklist bespreken we 5 aandachtspunten die leiden naar een veilige werkomgeving:

1. Voorkomen
2. Detecteren
3. Oplossen
4. Herstellen
5. Continue monitoring

Aandachtspunt 1: Voorkomen

'Voorkomen' is de eerste stap naar een veilige werkomgeving en bestaat eigenlijk uit twee delen:

A. Het inregelen van de juiste technologie

B. Bewustwording bij medewerkers

A) Inregelen van de juiste technologie
Het begint met het implementeren van de juiste technologie binnen je organisatie. Om chaos te verminderen, helpt een digitale werkomgeving waarin alles samenkomt wat je als medewerker nodig hebt. Je bestanden, documenten, apps, alles is terug te vinden in één online bureaublad.

Cloud oplossingen zijn vandaag de dag de veiligste manier om te werken dankzij de automatische beveiligingsupdates. Bovendien worden processen en security preventief gecheckt en indien nodig bijgewerkt, zonder dat je dat een volledige FTE kost. Bij een lokale server is dat handwerk en levert bijna altijd onderbrekingen en problemen op.

Naast security overwegingen, zijn er ook financiële. Cloud technologie is namelijk schaalbaar, waardoor je alleen betaalt wat je gebruikt en je geen investerings- en onderhoudskosten meer hebt.

Optimale informatiebeveiliging wordt op 3 niveaus ingeregeld. Denk als een crimineel, maak het ze zo moeilijk mogelijk. Als ze namelijk veel moeite moeten doen, gaan ze door naar het volgende adres waar het makkelijker is om binnen te komen:

- Bestanden en documenten
- Devices
- Eindgebruikers

Voorbeelden zijn oplossingen als MultiFactor Authentication (MFA), waarbij je naast een wachtwoord ook een code moet invoeren die je per sms toegestuurd krijgt. Of het encrypten van bestanden voordat je ze doorstuurt.

B) Bewustwording bij medewerkers
Zoals al eerder vermeld, wordt 60% van de datalekken en virus besmettingen veroorzaakt door een menselijke fout. Daarom is het ook zo belangrijk om je medewerkers te betrekken bij informatiebeveiliging van je organisatie. Creëer beleid over wat wel en niet gedownload mag worden. Zorg dat medewerkers de nieuwe technologie optimaal gebruiken en niet meer op zoek gaan naar onveilige alternatieven.

Checklist: Voorkomen

- ✔ Implementeer een digitale werkomgeving met Single Sign On
- ✔ Beveilig je organisatie op 3 niveaus: bestanden, devices, eindgebruikers
- ✔ Ga op zoek naar een oplossing die 3 niveaus in één keer kan beveiligen
- ✔ Creëer beleid voor medewerkers
- ✔ Zorg voor adoptie en training van nieuwe technologie voor medewerkers

Aandachtspunt 2: Detecteren

De tweede fase voor een veilige werkomgeving is het op tijd detecteren van nieuwe cyberdreigingen. Wil je dit adequaat realiseren, zonder dat je fulltime een medewerker hieraan kwijt bent, dan heb je de juiste technologie nodig die automatisch je processen en systemen scant. Dat gaat verder dan alleen het installeren van een virusscanner op je computer. Denk ook aan oplossingen als Advanced Threat Protection (ATP) waarmee email vooraf wordt gescand op schadelijke hyperlinks en bijlagen.

*Bron: Consumentenbond www.consumentenbond.nl/acties/updaten/veiligheidsupdates-android-toestellen-lopen-achter

Sowieso is het belangrijk om alle devices binnen je organisatie te beveiligen, dus ook smartphones die zakelijk gebruikt worden. Wist je dat ruim 25% van de Android smartphones nog een oude beveiligingsupdate heeft en kwetsbaar is voor hackers?[1] Veel organisaties staan er niet bij stil om deze ook te beveiligen. Dat kan centraal geregeld worden met een Mobile Device Management oplossing, waarmee je o.a. op afstand een smartphone kunt wissen, blokkeren en bepaalde applicaties kunt pushen.

Eén van de punten die opgenomen zou moeten worden in je security beleid: houd je smartphone up-to-date en download altijd de laatste updates die door je besturingssysteem worden gepusht.

Checklist: Detecteren

- ✔ Installeer security applicaties, zoals virusscanners en ATP
- ✔ Besteed extra aandacht aan de beveiliging van smartphones

Aandachtspunt 3: Oplossen

Ondanks alle beveiligingsmaatregelen die je hebt genomen, kan het gebeuren dat je toch getroffen wordt door een virus, malware of ransomware.

Met een digitale werkomgeving inclusief de juiste security technologie, worden werkplekken die toch geïnfecteerd zijn, geïdentificeerd en geïsoleerd. Wanneer je dan gehackt wordt, is dat maar bij één medewerker en ligt niet gelijk de hele organisatie plat. Infecties worden verwijderd, de betreffende werkplek wordt schoongeveegd en de medewerker kan weer aan de slag. Ook hier komen we weer terug op het feit dat technologie de sleutel is om dit adequaat in te regelen.

Checklist: Oplossen

- ✔ Installeer security applicaties, zoals virusscanners en ATP
- ✔ Regel support van een specialist als je zelf niet de kennis in huis hebt

Aandachtspunt 4: Herstellen

Herstellen is het vierde aandachtspunt voor een veilige werkomgeving. Mocht je toch getroffen zijn door een cyberaanval en is het opgelost? Dan is de volgende stap om processen, systemen en bestanden te herstellen. Een belangrijke stap om de continuïteit van je organisatie te waarborgen.

Voorwaarde is dat je een goede back-up hebt. Grofweg kun je back-ups op twee manieren regelen:

A. Een back-up met harde schijven e.d.

B. Met een cloud back-up

A) Back-up met harde schijven
Deze optie vereist handwerk en discipline. Vooral discipline om iedere dag te controleren of de back-up wel draait. Eén keer vergeten op een cruciaal moment en je kunt net die belangrijke offerte kwijt zijn wanneer je organisatie wordt getroffen door een cyberaanval. Bovendien moet je daarna handmatig de juiste back-up terug zetten en de rechten weer toekennen aan de juiste personen. Dit kost je organisatie al snel een FTE per week + onderhoudskosten voor de back-up.

B) Cloud back-up
Met een cloud back-up hoef je je daar geen zorgen over te maken. Je raadt het al, back-ups worden automatisch gedaan. Email, documenten, bestanden, alles wordt regelmatig opgeslagen op een veilige plaats in de cloud. En heb je de back-up nodig, dan is dat met een paar klikken geregeld, altijd, overal en vanaf elke device. Bovendien is een cloud back-up ook schaalbaar en kun je op die manier overcapaciteit eenvoudig voorkomen.

Checklist: Herstellen

- ✔ Bepaal hoe je de back-up wilt regelen: fysiek of in de cloud
- ✔ Implementeer de back-up methode
- ✔ Zorg voor een regelmatige back-up
- ✔ Maak een keuze: zelf doen of uitbesteden

Aandachtspunt 5: Continue monitoring

Misschien wel het belangrijkste aandachtspunt voor het creëren van een veilige werkomgeving: continue monitoring. Het voortdurend in de gaten houden of cyberaanvallen wegblijven en of medewerkers het security beleid naleven.

Deels is dit te automatiseren door bijvoorbeeld een externe partij in te schakelen die op de achtergrond je systemen in de gaten houdt. Aan de andere kant blijft het ook mensenwerk.

- Blijf medewerkers informeren over de nieuwste dreigingen
- Wees transparant over de gevolgen voor de organisatie (en indirect voor de medewerker zelf) wanneer je je niet houdt aan het opgestelde beleid
- Geef tips om de veilige werkomgeving in stand te kunnen houden

Door informatiebeveiliging op de agenda van de directie te zetten, blijft het een punt wat niet vergeten kan worden.

Bij veel organisaties zien we dat de eerste vier punten goed geregeld worden, en dat het stokt bij de monitoring. Zonde van je investeringen, want als je dan toch getroffen wordt door cyberaanval die voorkomen had kunnen worden, zit je alsnog met de gevolgen, zowel financieel als voor je reputatie.

Checklist: Continue monitoring

- Stel een proces op voor de continue monitoring
- Informeer medewerkers op regelmatige basis
- Zet informatiebeveiliging op de agenda van de directie
- Maak een keuze: zelf doen of uitbesteden?

Samengevat:
Checklist voor een veilige werkomgeving

- Implementeer een digitale werkomgeving, zoals Office 365
- Beveilig je organisatie op 3 niveaus: bestanden, devices, eindgebruikers
- Creëer beleid voor medewerkers
- Zorg voor Adoptie en training van nieuwe technologie voor medewerkers
- Installeer security applicaties, zoals virusscanners en ATP
- Besteed extra aandacht aan de beveiliging van smartphones
- Zorg voor een regelmatige (cloud) back-up
- Stel een proces op voor de continue monitoring
- Informeer medewerkers op regelmatige basis over informatiebeveiliging
- Zet informatiebeveiliging op de agenda van de directie
- Maak een keuze: zelf doen of uitbesteden

Conclusie:

Het moment is nú om een veilige werkomgeving te implementeren binnen je organisatie. Zorg dat je informatiebeveiliging gestructureerd aanpakt voor het beste resultaat op de langere termijn.
Met cyberdreigingen die steeds geavanceerder worden en de invoering van de GDPR, is nu het momentum aangebroken om kritisch naar de informatiebeveiliging van je organisatie te kijken. Nieuwe technologieën kunnen je helpen om de security relatief eenvoudig en gedegen te realiseren.

Een digitale werkomgeving heeft ook invloed op de financiële balans van de organisatie: de werkomgeving gaat van Capex naar Opex op je balans. In plaats van dat je in één keer flink moet investeren in een server op locatie die relatief snel veroudert en handmatig onderhouden moet worden, stap je over op een schaalbare, veilige cloud oplossing. Op- en afschalen is geen probleem, je betaalt alleen wat je daadwerkelijk gebruikt, en koopt alleen de licenties die je nodig hebt. Server capaciteit on demand dus, waardoor je nooit met kostbare overcapaciteit zit.

Zorg dat je organisatie cybercrime proof is

Wil je weten hoe INTO kan helpen om de veilige werkomgeving te creëren voor jouw organisatie? De consultants van INTO denken graag met je mee en laten je de beste opties zien. Neem contact met ons op voor een vrijblijvend adviesgesprek.

www.into.nu/contacteer-mij/

088 - 7777 010

marketing@into.nu

Over INTO
INTO is de grootste B2B leverancier van Nederland voor Telecom en Cloud Based werkomgevingen. Wij begeleiden je organisatie in het digitale transformatieproces voor vandaag en morgen. Dat doen we door bouwblokken aan te bieden voor een digitale werkomgeving voor telecom en IT, inclusief de bijbehorende infrastructuur.

Samen met jou gaan we op zoek naar innovatieve oplossingen, waarbij transparantie en toegankelijkheid centraal staan. ‘Simplicity as a Service’ noemen we dat. INTO kan je medewerkers nog slimmer laten samenwerken dankzij onze nauwe samenwerking met Triple A partners en 45 krachtige franchiseondernemers. Zij zijn verspreid over heel Nederland zodat zij ervoor kunnen zorgen dat je organisatie zich kan concentreren op waar je goed in bent: ondernemen!