IRIS ONE ICT

Hoe veilig is jouw mkb-organisatie

In 11 stappen je cybersecurity op orde

Een dag geen e-mail? Per ongeluk adreslijsten naar het verkeerde e-mailadres verstuurd? Of zijn je bestanden gegijzeld door gijzelsoftware? Je IT moet het altijd doen en cybersecurity is belangrijker dan ooit. Met deze checklist neutraliseer je de belangrijkste gevaren voor jouw onderneming.

Zeker de helft van de mkb-bedrijven heeft last van cybercriminaliteit. En toch neemt slechts de helft van de ondernemers voldoende (basis)maatregelen om zich te beschermen tegen cybercriminelen en de data goed te beveiligen. We werkten al relatief veel digitaal, de coronacrisis gaf dat nog een enorme boost. En dat bleken hoogtijdagen voor hackers. Na een aanval met ransomware, maar ook na brand of waterschade, wil je binnen een paar uur toch weer volledig aan de slag kunnen.

Eigen mensen het grootste cybergevaar

Alles technisch dichtspijkeren kan, maar daarmee ben je er nog zeker niet. Datalekken komen bij de beste bedrijven voor en meestal ligt er een menselijke fout aan ten grondslag. Klikken op phishing mails of een onbeveiligde smartphone kwijtraken, het gebeurt regelmatig. Cybersecurity is dus een samenspel van de juiste technische tools en bewustzijn bij ál je collega's. Er hoeft maar één iemand in de fout te gaan en voor je het weet worden inlogcodes van jouw bedrijf verkocht op het internet. Met deze checklist maak je je systemen veilig en help je je collega's veiliger werken.

Maak iedereen bewust van cyberveiligheid

Het grootste cybergevaar is nietsdoen. Maak concrete afspraken wie verantwoordelijk is voor de cyberveiligheid. Bedenk iets ludieks om elkaar aan de afspraken te houden. Degene die zijn werkplek achterlaat zonder de computer te vergrendelen mag trakteren! Iedereen maakt fouten, straf ze daarom niet af, maar hou het luchtig en coach elkaar. Op die manier durven mensen hun fouten toe te geven, waardoor je bijtijds de juiste maatregelen treft. Maak de afspraken niet per mail, maar praat regelmatig met collega's over veilig werken en check of hun werkroutines ook echt veilig zijn.

Bescherm jezelf tegen fraudemails

Ook wel eens op een e-mail geklikt met dubieuze inhoud? Je bent niet de enige! Fraudemails zijn tegenwoordig amper van legitieme e-mails te onderscheiden. Je hebt het druk én een volle inbox, hierdoor trapt menig ondernemer in de val. Neem altijd de tijd om een e-mail goed te lezen en vraag ook je collega's dat te doen, voordat ze ergens op klikken. Het scheelt dat Microsoft 365 al je e-mails analyseert en vooraf verdachte URL's eruit filtert, nog voordat je erop klikt. En onveilige bijlagen gaan direct in quarantaine. Staat er een gevaarlijke link in een e-mail, dan waarschuwt het systeem. Op deze manier kan het niet fout gaan. Blijf desondanks altijd op je hoede en klik bij twijfel niet!

Maak gebruik van multi-factor authenticatie

Wachtwoorden onthouden en overal invoeren is vervelend. Je hebt er ook zo veel. Daarom kiezen ook veel ondernemers gemakkelijk te onthouden - en te achterhalen - wachtwoorden. Dit soort wachtwoorden resulteert in 91% van alle geslaagde cyberinbraken. Inloggen met wachtwoorden is echt niet meer van deze tijd; het inloggen via gezichtsherkenning of via een vingerafdruk is inmiddels gemeengoed geworden. Denk maar aan inloggen in Windows 10 via gezichtsherkenning, het ontgrendelen van je telefoon met een vingerafdruk of het openen van jouw favoriete bank-app met Face ID. Hoog tijd dus om ook op de zaak te kiezen voor een veiligere manier van inloggen met multi-factor authenticatie. Wil je inloggen, dan bewijs je met een vingerafdruk, token of melding naar een mobiele telefoon dat je het echt bent.

Stel interne netwerkbeveiliging in

Hackers houden zich vaak lang verscholen en gaan stilletjes te werk. Ze zoeken bestanden en kopiëren ze zonder zich te laten zien of direct losgeld te eisen. Ontmasker deze types en voorkom erger met automatische analyses. Office 365 Advanced Threat Protection (ATP) checkt wie er inlogt en hoe ze zich gedragen. Logt er iemand eerst in Heerenveen in en een uur later in China? Kopieert iemand ineens grote hoeveelheden data? Dan ontzegt ATP automatisch de toegang en stuurt een wachtwoord- reset.

Krijg weer grip op je bestanden

Bestanden staan op de kantoorserver, op smartphones en in de cloud. Heb jij soms ook het gevoel dat je de grip op data kwijt bent? Microsoft 365 vindt, classificeert en versleutelt al je bestanden. Sta je op het punt privacygevoelige informatie te delen? Dan krijg je een seintje waardoor je niet meer in de fout hoeft te gaan. Zo voorkom je dat de Autoriteit Persoonsgegevens voor de deur staat omdat je in overtreding bent met de AVG. Zijn collega's hun smartphone kwijt? Dan wis je op afstand alle bedrijfsbestanden, dit is wel zo veilig. Gaat iemand uit dienst? Dan deactiveer je zijn of haar licentie zodat hij of zij geen toegang meer heeft tot applicaties en bestanden.

Al je software up-to-date

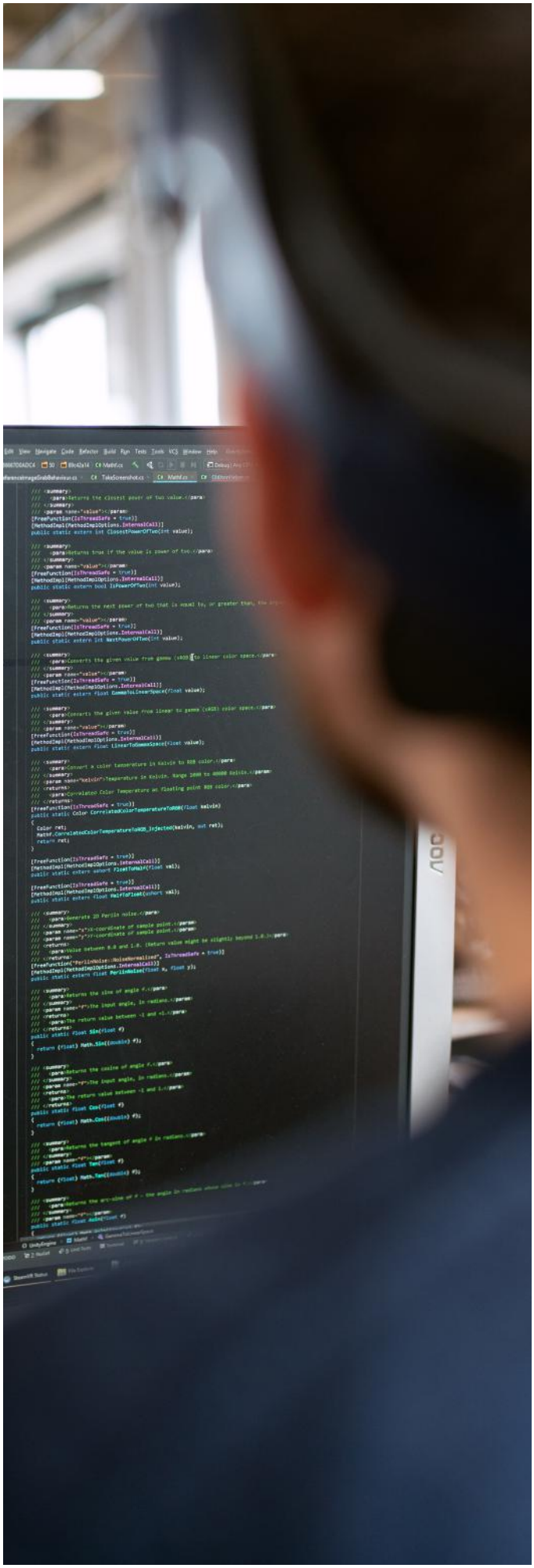
Zijn al je apps wel up-to-date? Software die niet de laatste update heeft gekregen, vormt een beveiligingsgevaar voor je hele netwerk. Via open achterdeurtjes sluipen de cybercriminelen naar binnen. Check daarom al je apps en kantooroplossingen. Het kan zijn dat je nog met verouderde systemen werkt die geen update meer krijgen. Het is dan verstandig om die te vervangen door moderne, wel goed beveiligde tools. Denk bijvoorbeeld aan alle tools van Microsoft die in de cloud staan. Hier worden veiligheidsupdates automatisch geïnstalleerd en werk je altijd veilig. Geef computers ook de kans om updates te draaien. Negeer updates niet, stel ze niet uit en herstart je computer zo nu en dan zodat de updates ook echt geïnstalleerd worden.

Al je hardware up-to-date

Niet alleen software, maar ook hardware heeft soms een achterdeur openstaan. Alle apparaten die aan het netwerk hangen zoals printers, internetradio's, routers en switches moeten zo nu en dan een update krijgen om echt veilig te zijn. Veel apparaten voeren die automatisch door, maar vooral oudere toestellen niet. Check al je apparatuur en durf ook afscheid te nemen van die oude, onveilige apparatuur.

Back-ups geregeld

Sla regelmatig je gegevens op en laat ook die automatisch back-uppen. Op die manier raak je niets kwijt en kun je na een calamiteit weer snel door. Microsoft 365 slaat niet automatisch al je bestanden voor langere tijd op. Kijk daarom naar de mogelijkheden voor automatische back-ups.



Versleutel je gegevens

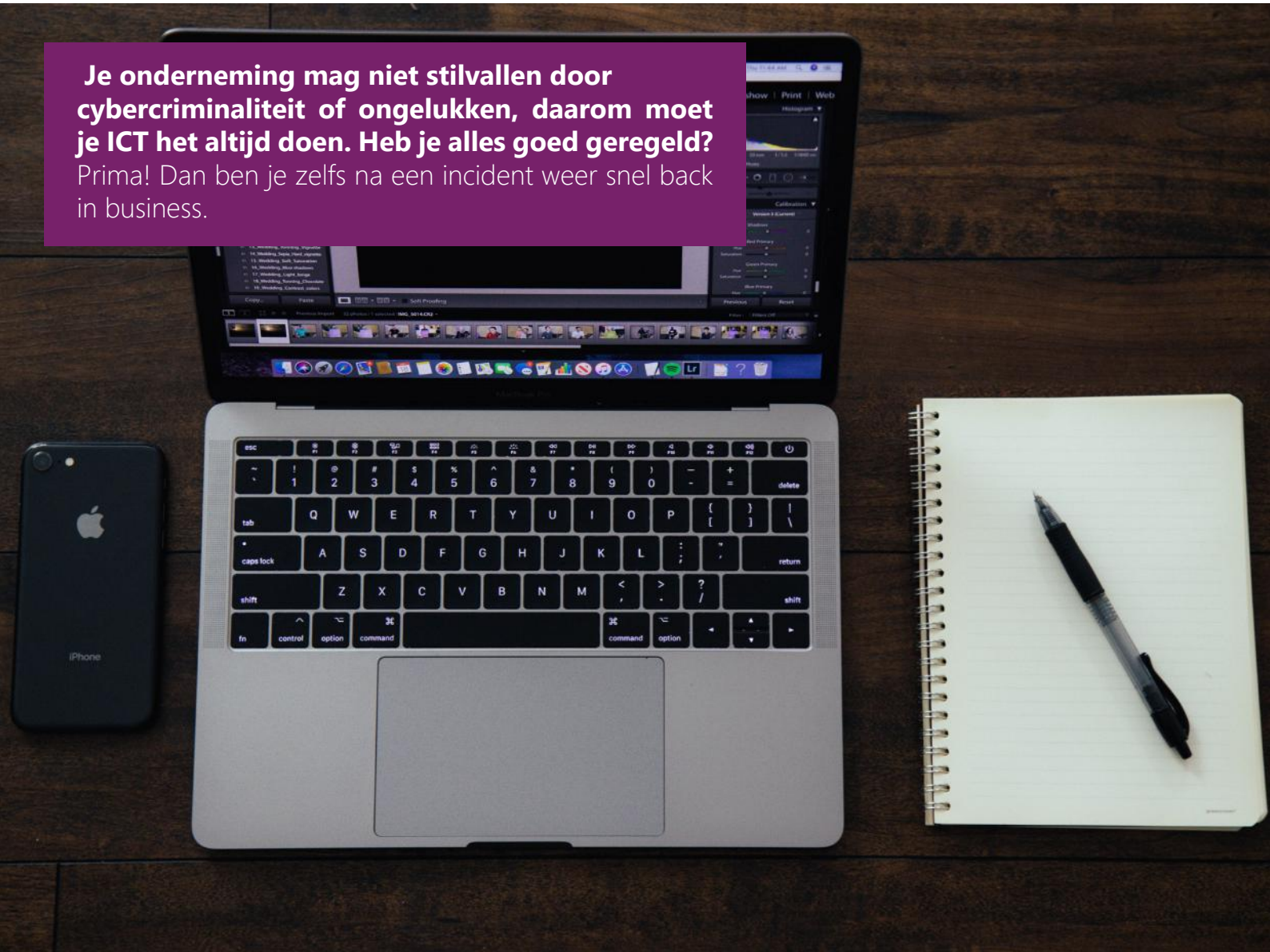
Of gegevens in de cloud, op telefoons of op computers staan, ze kunnen in verkeerde handen vallen. Een cruciale stap is om gegevens via encryptie (versleuteling) te beveiligen. BitLocker versleutelt alle bestanden. Een gestolen harde schijf is dan in de handen van criminelen onbruikbaar.

Alle devices goed beveiligen

Je ziet nog steeds dat sommige telefoons en computers opstarten zonder dat een wachtwoord of pincode wordt gevraagd. Stel dit zo snel mogelijk in. Met Microsoft Endpoint Manager houd je centraal regie over alle apparaten. Je installeert de recentste beveiligingsmaatregelen bij verlies en bij diefstal verwijder je de bedrijfsgegevens.

Geef security uit handen

Cybersecurity vraagt om specialistische IT-kennis. Dat is voor mkb'ers zelf niet optimaal te regelen. Daarom kiezen steeds meer ondernemers ervoor om het uit handen te geven. Hierdoor ben je ook buiten kantooruren optimaal beschermd doordat het netwerk continu in de gaten wordt gehouden. Je hoeft niet meer te denken aan back-ups, updates, beveiligingspatches, trainingen en regelmatige netwerktesten want onze specialisten nemen je dit werk uit handen. Zo kun jij je volledig focussen op de zaak



Je onderneming mag niet stilvallen door cybercriminaliteit of ongelukken, daarom moet je ICT het altijd doen. Heb je alles goed geregeld? Prima! Dan ben je zelfs na een incident weer snel back in business.

IRIS ONE ICT

Graafsebaan 111,
5248 NL Rosmalen
073 523 2288
iris@iris-one.nl
www.iris-one.nl

Het maximale uit jezelf halen, iedere dag.