enisa

AGENTSCHAP VAN DE EUROPESE UNIE VOOR CYBERBEVEILIGING

Leidraad cyberbeveiliging voor kmo's

12 STAPPEN VOOR EEN VEILIG BEDRIJF

De COVID-19-crisis heeft duidelijk gemaakt hoe belangrijk het internet en computers in het algemeen zijn voor kmo's. Om de continuïteit van hun bedrijf veilig te stellen en tijdens de pandemie fatsoenlijk te kunnen blijven meedraaien, zagen veel kmo's zich genoodzaakt maatregelen te nemen door bijvoorbeeld clouddiensten in te voeren, de internetdiensten te verbeteren, hun website te vernieuwen en het personeel op afstand te laten werken.

In deze folder wordt in twaalf praktische stappen weergegeven hoe kmo's hun systemen en hun bedrijf beter kunnen beveiligen. Deze uitgave hoort bij het meer gedetailleerde Enisa-verslag **"Cybersecurity for SMEs – Challenges and Recommendations"** (cyberbeveiliging voor kmo's – uitdagingen en aanbevelingen).

1 EEN GOEDE CULTUUR VOOR CYBERBEVEILIGING

VERANTWOORDELIJKHEID VOOR BEHEER

Optimale cyberbeveiliging is voor iedere kmo onmisbaar met het oog op blijvend succes. De verantwoordelijkheid voor deze kritieke functie moet worden toegewezen aan iemand binnen de organisatie die ervoor zorgt dat aan cyberbeveiliging de benodigde middelen worden toegekend, zoals arbeidstijd, software, diensten en hardware voor cyberbeveiliging, personeelsopleiding en doeltreffend beleid.

DRAAGVLAK BIJ WERKNEMERS

Creëer een draagvlak bij uw werknemers via doeltreffende communicatie over cyberbeveiliging vanuit het management, waarbij leidinggevenden initiatieven voor cyberbeveiliging openlijk steunt, werknemers passende opleiding krijgen en duidelijke, specifieke voorschriften worden vastgelegd in cyberbeveiligingsbeleid.

CYBERBEVEILIGINGSBELEID

Publiceer een cyberbeveiligingsbeleid met duidelijke, specifieke voorschriften over het verwachte gedrag van werknemers bij gebruik van de ICT-omgeving, -apparatuur en -diensten van de onderneming. Hierin moeten ook de mogelijke gevolgen worden beschreven voor werknemers die zich niet aan de voorschriften houden. Het beleid moet periodiek worden herzien en bijgewerkt.

CYBERBEVEILIGINGSCONTROLES

Laat periodiek cyberbeveiligingscontroles uitvoeren door controleurs die beschikken over de nodige kennis, vaardigheden en ervaring. De controleurs moeten onafhankelijk zijn, of zij nu extern worden ingehuurd dan wel interne werknemers van de kmo zijn die losstaan van de dagelijkse IT-activiteiten.

OOG VOOR GEGEVENSBESCHERMING

In de AVG[1] is bepaald dat kmo's die persoonsgegevens van ingezetenen van de EU/EER verwerken of opslaan, die gegevens moeten beschermen met passende beveiligingscontroles. Zij dienen er ook op toe te zien dat derden die werk voor hen verrichten, passende beveiligingsmaatregelen toepassen.

[1] Algemene verordening gegevensbescherming, https://ec.europa.eu/info/law/law-topic/data-protection_en

2

PASSENDE OPLEIDING

Bied periodiek opleidingen in cyberbewustzijn aan voor al uw werknemers, zodat zij de diverse cyberdreigingen kunnen herkennen en afweren. Die opleidingen moeten op kmo's zijn afgestemd en gericht zijn op levensechte situaties.

Zorg voor gespecialiseerde opleidingen voor de verantwoordelijken voor cyberbeveiligingsbeheer in uw onderneming, zodat zij over de vaardigheden en competenties beschikken die zij nodig hebben voor hun werk.

3

EFFECTIEF DERDENBEHEER

Zorg ervoor dat alle leveranciers, met name als zij toegang hebben tot gevoelige gegevens en/of systemen, actief worden beheerd en voldoen aan de overeengekomen beveiligingsniveaus. Leg contractueel vast op welke wijze leveranciers aan die beveiligingseisen voldoen.

4

RESPONSPLAN VOOR INCIDENTEN

Stel een formeel incidentenresponsplan op, met duidelijke en gedocumenteerde richtsnoeren, taken en verantwoordelijkheden, zodat op alle beveiligingsincidenten tijdig, professioneel en passend wordt gereageerd. Probeer hulpprogramma's te vinden die verdachte activiteit of beveiligingsinbreuken opsporen en waarschuwingen genereren, zodat een snelle respons mogelijk is.

5 BEVEILIGDE TOEGANG TOT SYSTEMEN

Zet iedereen aan tot het gebruik van een wachtzin, een reeks van drie of meer willekeurige algemene woorden die samen een zin vormen en die zowel gemakkelijk te onthouden als moeilijk te raden zijn.

Als u voor een typisch wachtwoord kiest:

- Bedenk dan een lang wachtwoord met hoofd- en kleine letters, en eventueel cijfers en speciale tekens.
- Vermijd voor de hand liggende woorden, zoals "wachtwoord", en letter- of cijferreeksen zoals "abc" of "123".
- Vermijd het gebruik van persoonlijke informatie die online te vinden is.

Of u nu wachtzinnen of wachtwoorden gebruikt:

- Gebruik ze ergens anders niet opnieuw.
- Deel ze niet met collega's.
- Schakel multifactorauthenticatie in.
- Gebruik een speciale wachtwoordmanager.

6

BEVEILIGDE APPARATUUR

Het beveiligen van de apparatuur die in gebruik is bij het personeel, of het nu gaat om pc's, laptops, tablets of smartphones, is een essentiële stap in een cyberbeveiligingsprogramma.

TIJDIGE PATCHES EN UPDATES VOOR SOFTWARE

Gebruik voor het patchbeheer bij voorkeur een gecentraliseerd platform. Wij bevelen kmo's ten zeerste aan om:

- al hun software regelmatig te updaten;
- waar mogelijk automatische updates in te schakelen;
- na te gaan welke software en hardware handmatig moet worden geüpdatet;
- rekening te houden met mobiele en IoT-apparatuur.

BESCHERMING TEGEN VIRUSSEN

Bescherm alle apparaten met de laatste versie van een centraal beheerde antivirusoplossing, zodat de goede werking ervan wordt gewaarborgd. Installeer geen illegale software, want die kan malware bevatten.

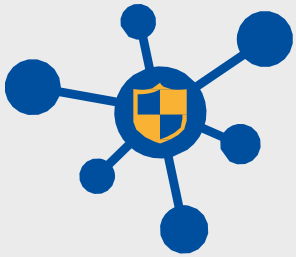
HULPPROGRAMMA'S VOOR DE BESCHERMING VAN E-MAILS EN INTERNETVERKEER

Maak gebruik van oplossingen om spam, e-mails met links naar kwaadaardige websites, e-mails met kwaadaardige bijlagen zoals virussen en phishing-e-mails te blokkeren.

VERSLEUTELING

Bescherm uw gegevens door middel van versleuteling. Kmo's moeten erop toezien dat opgeslagen gegevens op mobiele apparaten zoals laptops, smartphones en tablets worden versleuteld. Zorg er daarom voor dat via openbare netwerken – zoals de wifi van hotels of luchthavens – verzonden gegevens gecodeerd zijn, hetzij door gebruik te maken van een virtueel particulier netwerk (VPN), hetzij door websites te bezoeken via beveiligde verbindingen met het SSL/TLS-protocol. Zie er ook op toe dat de gegevens van uw klanten bij verzending via uw eigen website worden beschermd met geschikte encryptietechnologie.

7 BEVEILIGD NETWERK



BEHEER VAN MOBIELE APPARATEN

Veel kmo's laten medewerkers die op afstand werken, gebruikmaken van hun eigen laptop, tablet en/of smartphone. Daardoor kan er een beveiligingsrisico ontstaan voor gevoelige bedrijfsgegevens op die apparatuur. Dat risico kan onder meer worden ondervangen door een oplossing voor het beheer van mobiele apparaten te implementeren, waarmee kmo's kunnen:

- bepalen welke apparaten toegang krijgen tot hun systemen en diensten;
- garanderen dat het apparaat is voorzien van de meest recente antivirussoftware;
- nagaan of het apparaat is versleuteld;
- controleren of op het apparaat de laatste patches zijn geïnstalleerd;
- bepalen dat het gebruik van het apparaat afhankelijk is van bescherming met een pincode en/of wachtwoord;
- zorgen dat op afstand bedrijfsgegevens worden gewist als de eigenaar het apparaat als verloren of gestolen opgeeft of uit dienst treedt bij de onderneming.

FIREWALLS

Een firewall beheert het inkomend en uitgaand verkeer over een netwerk en is cruciaal voor de bescherming van de systemen van kmo's. Bescherm al uw bedrijfskritieke systemen met een firewall en installeer met name een firewall tussen uw netwerk en het internet.

OPLOSSINGEN VOOR TOEGANG OP AFSTAND

Kmo's moeten regelmatig nagaan of hun middelen voor toegang op afstand veilig zijn, en met name:

- erop toezien dat alle software voor toegang op afstand gepatcht en up-to-date is;
- de toegang vanaf verdachte geografische locaties of bepaalde IP-adressen blokkeren;
- personeel op afstand alleen toegang verlenen tot de systemen en computers die zij nodig hebben voor hun werk;
- sterke wachtwoorden verplicht stellen en waar mogelijk multifactorauthenticatie inschakelen;
- zorgen voor controle op en waarschuwing bij vermoedelijke aanvallen of ongebruikelijke, verdachte activiteit.

8 BETERE FYSIEKE BEVEILIGING

Overal waar zich belangrijke informatie bevindt, zijn passende fysieke controles onontbeerlijk. Zo mag een laptop of smartphone van het werk niet onbewaakt op de achterbank van een auto blijven liggen. Medewerkers moeten hun computer steeds vergrendelen wanneer er niet op aan het werk zijn. U kunt ook de automatische vergrendelfunctie inschakelen op ieder apparaat dat in gebruik is voor bedrijfsdoeleinden. Hetzelfde geldt voor gevoelige gedrukte documenten: laat ze niet onbeheerd achter maar berg ze veilig op wanneer ze niet worden gebruikt.

9 BEVEILIGDE BACK-UPS

Om belangrijke informatie te kunnen herstellen, moeten er back-ups worden bijgehouden. De informatie kan dan doeltreffend worden hersteld na bijvoorbeeld een ransomwareaanval. Volg daarbij de volgende regels:

- de back-up wordt regelmatig en waar mogelijk automatisch uitgevoerd,
- de back-up wordt apart gehouden van de productieomgeving van het bedrijf,
- de back-up wordt versleuteld, vooral bij verplaatsing tussen locaties,
- er vinden regelmatig tests plaats om te verifiëren dat herstel van gegevens uit de back-up mogelijk is. Bij voorkeur wordt er regelmatig getest op volledig herstel van begin tot eind.

10 CLOUDDIENSTEN

Hoewel cloudoplossingen veel voordelen bieden, brengen zij ook enkele unieke risico's met zich mee. Kmo's doen er goed aan die in acht te nemen alvorens in zee te gaan met een cloudprovider. Enisa heeft voor kmo's die naar de cloud migreren een handleiding gepubliceerd: "Cloud Security Guide for SMEs"[2].

Bij het maken van hun keuze moeten kmo's nagaan of de cloudprovider de wet- of regelgeving niet overtreedt door gegevens – met name persoonsgegevens – op te slaan buiten de EU/EER. In de AVG staat bijvoorbeeld dat persoonsgegevens van inwoners binnen de EU/EER alleen onder zeer specifieke voorwaarden buiten de EU/EER mogen worden opgeslagen of doorgegeven.

[2] https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

11 VEILIGE WEBSITES

Het is van essentieel belang dat kmo's ervoor zorgen dat hun website veilig wordt geconfigureerd en onderhouden en dat alle persoons- en financiële gegevens, zoals creditcardgegevens, goed beschermd zijn. Dat houdt in dat zij de beveiliging van hun website regelmatig testen om eventuele zwakke plekken vast te stellen, en dat zij regelmatig controleren of de website goed wordt onderhouden en bijgewerkt.

12 INFORMATIE ZOEKEN EN DELEN

Een doeltreffende manier om cybercriminaliteit te bestrijden, is het delen van informatie. Door informatie op het gebied van cybercriminaliteit uit te wisselen, krijgen kmo's namelijk meer inzicht in de risico's waarmee zij te maken hebben. Ondernemingen zullen eerder geneigd zijn actie te ondernemen om hun systemen te beveiligen als zij rechtstreeks van branchegenoten horen welke problemen met cyberbeveiliging er bestaan en hoe die zijn opgelost, dan wanneer zij daarover lezen in sectorverslagen of onderzoeken naar cyberbeveiliging.

AGENTSCHAP VAN DE EUROPESE UNIE VOOR CYBERBEVEILIGING

OVER ENISA

Het Agentschap van de Europese Unie voor cyberbeveiliging, Enisa, streeft ernaar een hoog niveau van cyberbeveiliging in heel Europa te bereiken. Enisa is opgericht in 2004 en heeft een sterker fundament gekregen door de cyberbeveiligingsverordening van de EU. Het Agentschap draagt bij aan het cyberbeveiligingsbeleid van de EU, vergroot de betrouwbaarheid van ICT-producten, -diensten en -processen door middel van certificeringsprogramma's voor cyberbeveiliging, werkt samen met de lidstaten en instanties van de EU en helpt Europa zich voor te bereiden op de cyberuitdagingen van morgen. Door middel van kennisdeling, capaciteitsopbouw en bewustmaking werkt Enisa samen met zijn belangrijkste belanghebbenden om het vertrouwen in de verbonden economie te versterken, de veerkracht van de infrastructuur van de Unie te vergroten en uiteindelijk de Europese samenleving en burgers digitaal veilig te stellen. Ga voor meer informatie naar www.enisa.europa.eu.

Enisa
Agentschap van de Europese Unie voor cyberbeveiliging

Kantoor Athene
Ethnikis Antistaseos 72 &
Agamemnonos 14,
Chalandri 15231, Attiki, Griekenland

Kantoor Heraklion
95 Nikolaou Plastira
700 13 Vassilika Vouton,
Heraklion, Griekenland

enisa.europa.eu