Security Gids

De 5 meest gemaakte fouten in IT-beveiliging
én tips voor een ijzersterke IT-beveiliging

ISSYS ICT

De 5 meest gemaakte fouten in IT-beveiliging

IT-beveiliging staat de laatste jaren hoog op de agenda. Toch loopt het nog regelmatig mis: een op de vijf mkb-bedrijven viel al eens ten prooi aan cybercriminaliteit. En 58 procent van alle inbreuken vindt plaats in het mkb. Bovendien steekt ransomware of gijzelsoftware vaker de kop op in Europa dan elders in de wereld. Sinds de komst van de nieuwe GDPR is het belangrijk om elk risico onder controle te houden. Veel mkb-ondernemers doen wat ze kunnen om kwaadwillige en onopzettelijke datalekken te dichten of te voorkomen. Dat lukt vaak niet omdat hun IT-beveiliging tekortschiet. De jouwe ook?

Ontdek de vijf meest gemaakte fouten in IT-beveiliging:

1

MENSELIJKE FOUT

Menselijke fouten vormen veruit de grootste bedreiging voor je beveiliging: 80 procent van de incidenten is daarvan het gevolg. Medewerkers openen kwaadaardige bijlagen of klikken op verkeerde links die leiden tot ransomware, virussen, … Of ze mailen naar de verkeerde ontvanger door een foutief e-mailadres te gebruiken of door een bestand per ongeluk te forwarden. Datalekken zijn niet alleen digitaal. Medewerkers printen soms bedrijfsgegevens en laten die rondslingeren bij de printer of op hun bureau. Zo komen ze vaak in de verkeerde handen terecht.

2

ONOPLETTENDHEID

Hoewel bijna iedereen zijn smartphone vergrendelt met een wachtwoord of code, vingerafdruk of gezichtsherkenning, vergeten de meeste mkb-ondernemers dat te regelen voor hun bedrijfssystemen. Zo kunnen medewerkers toegang krijgen tot de bedrijfsgegevens op onveilige apparaten zoals externe – misschien zelfs openbare – computers, persoonlijke mobiele telefoons, … Verlaten ze even hun werkplek? Dan vergrendelen ze hun computer vaak niet. En dat meerdere keren per dag. Ondertussen lopen buitenstaanders langs. Of nemen tijdelijke externen plaats aan de dichtstbijzijnde pc. Conclusie: mkb-ondernemers hebben nauwelijks controle over wie op welke toestellen werkt, en wat ze met die kostbare gegevens doen.

3 HALFBAKKEN VOORBEREIDING

Je waant je veilig want je systemen maken regelmatig een back-up van al je gegevens. En je hebt antivirussoftware, spamfilters en een firewall geïnstalleerd. Maar … werkt alles zoals jij denkt? Veel mkb-bedrijven installeren tal van beveiligingssystemen, zonder ze te testen. Faalt er een? Dan loopt het ondanks al die moeite en investeringen tóch mis:

- Ze worden het slachtoffer van cybercriminaliteit: virus, ransomware, …
- Er gaat kostbare informatie verloren.
- Onbevoegden – misschien zelfs concurrenten – krijgen gevoelige informatie in handen.

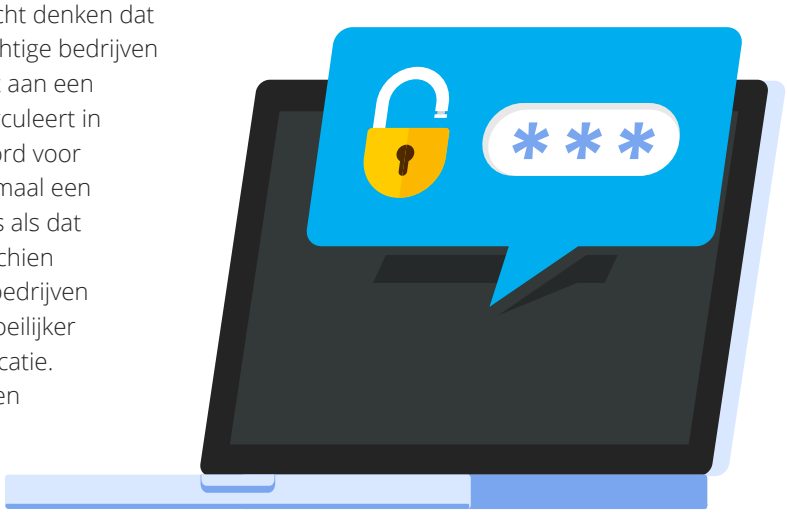
De gevolgen zijn desastreus. Het kost je veel geld en tijd om het virus of de ransomware te verwijderen. Zijn er persoonlijke gegevens van klanten gelekt? Dan kun je boetes krijgen tot 2% van je jaaromzet voor inbreuken op de GDPR. Je verliest je concurrentievoordeel als andere bedrijven met jouw ideeën aan de haal gaan. Bovendien lijdt je reputatie er onder en lopen je klanten over naar je concurrenten.

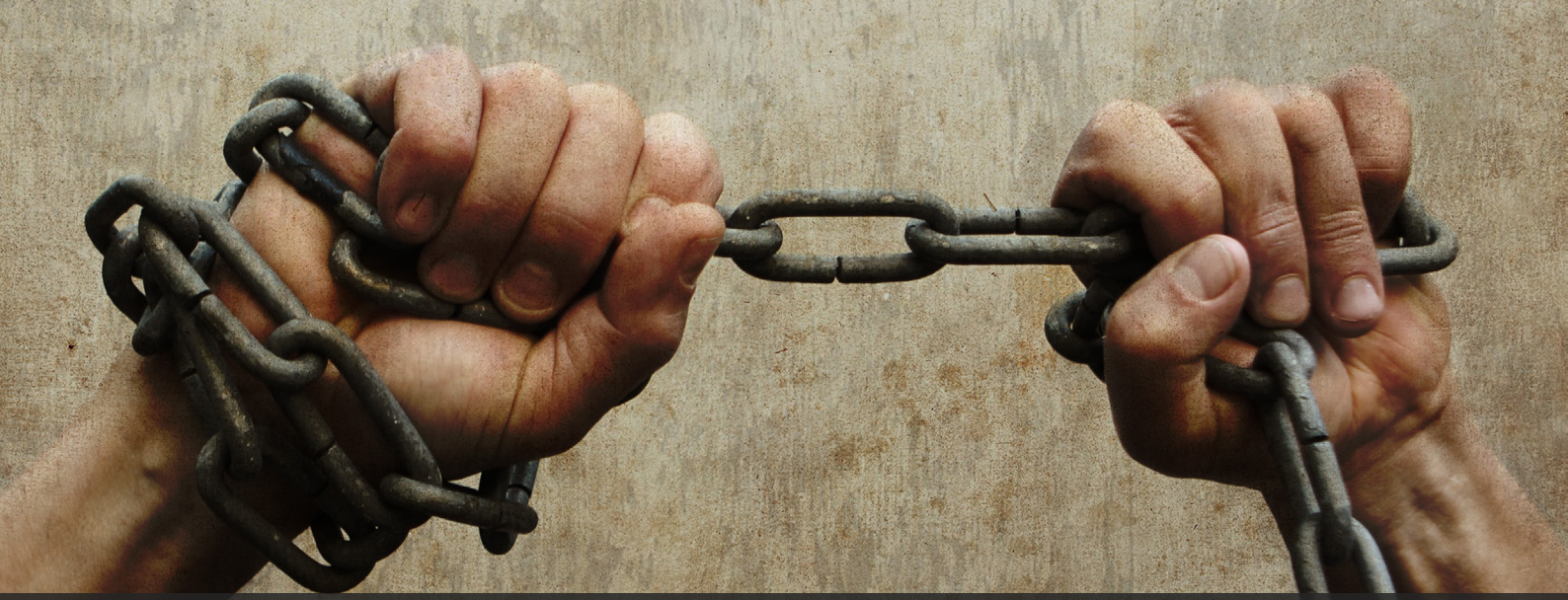
4 GEEN NOODPLAN

Wat doe jij bij een cyberaanval? Veel mkb-ondernemers hebben daar nog nooit bij stilgestaan. De meeste nemen wel maatregelen om aanvallen te voorkomen, maar bedenken geen processen om ze op te lossen. Doet zich een aanval voor? Dan weten velen niet meteen hoe ze moeten reageren en verliezen ze kostbare tijd. Ze nemen snel enkele beslissingen die ze ter plaatse – vaak in paniek – verzinnen. Omdat ze er nooit uitvoerig over hebben nagedacht en doorgaans geen uitgebreide IT-kennis hebben, zijn dat niet altijd de juiste beslissingen. Resultaat: het bedrijf ligt onnodig lang stil, met alle gevolgen van dien.

5 ONTOEREIKEND WACHTWOORDBELEID

Omdat mkb-ondernemers vaak onterecht denken dat datalekken vooral grote en kapitaalkrachtige bedrijven treffen, besteden ze te weinig aandacht aan een sterk en veilig wachtwoordbeleid. Zo circuleert in veel mkb-bedrijven hetzelfde wachtwoord voor alle medewerkers. Of ze gebruiken allemaal een eigen wachtwoord, dat vaak hetzelfde is als dat van hun persoonlijke account, dat misschien gehackt is. Daarnaast zetten te weinig bedrijven in op meervoudige authenticatie die moeilijker te hacken is dan enkelvoudige authenticatie. Cybercriminelen zijn zich van al die zaken bewust. Daarom richten ze zich steeds vaker op mkb-bedrijven.





Ga voor een ijzersterke IT-beveiliging

De tijd dat je je in een fort waande dankzij je firewall, antivirussoftware en spamfilters is voorbij. Tegenwoordig liggen er overal hackers op de loer die gaten in je beveiliging vinden of forceren. Maak je een of meer van de vijf meest gemaakte fouten? Dan is het dringend tijd om die aan te pakken. Want van dit soort fouten leer je liever niet. Roep hackers en onbedoelde datalekken een halt toe met een ijzersterke beveiliging.

BEPERK MENSELIJKE FOUTEN

Medewerkers lekken belangrijke gegevens meestal per ongeluk, en ontdekken dat vaak pas veel later. Leer hen waarop ze moeten letten, wat veilig is en wat niet. Dan klikken ze niet zonder na te denken op iedere link en dubbelchecken ze iedere geadresseerde. Maar mensen blijven … mensen, en die maken nu eenmaal fouten. Speel dus op zeker: kies software die fouten helpt voorkomen, zoals Microsoft 365. De functie Advanced Threat Protection scant en controleert automatisch alle bijlagen en links in e-mails. Zelfs als iemand toch op een onveilige link klikt, gaat het nog goed.

NEEM DE CONTROLE

Ben je het overzicht over je IT kwijt? Microsoft 365 wijst je de weg. Je bepaalt zelf wie welke gegevens mag openen of opslaan én op welke apparaten. Je beheert de toegang tot alle apparaten. Is er een zoek? Dan trek je die toegang eenvoudig weer in. Zo maken dieven geen enkele kans. In M365 stel je veiligheidsprocedures in zodat je medewerkers bijlagen bijvoorbeeld wel kunnen openen op mobiele apparaten, maar niet kunnen opslaan. Zo heb je je IT altijd volledig onder controle.

TEST, TEST EN TEST

Heb je een firewall, antivirussoftware en spamfilters? Prima! Controleer zeker of ze hun taak goed doen. Hoe? Met een penetratie- of binnendringtest onderzoek je of je systemen bestand zijn tegen kwaadwillige hackers. Zo breng je kwetsbaarheden aan het licht waarmee je dan aan de slag gaat. Houd je het liever eenvoudig? Microsoft 365 beschermt je systemen tegen cyberaanvallen en beveiligt al je gegevens.

BEREID JE GOED VOOR

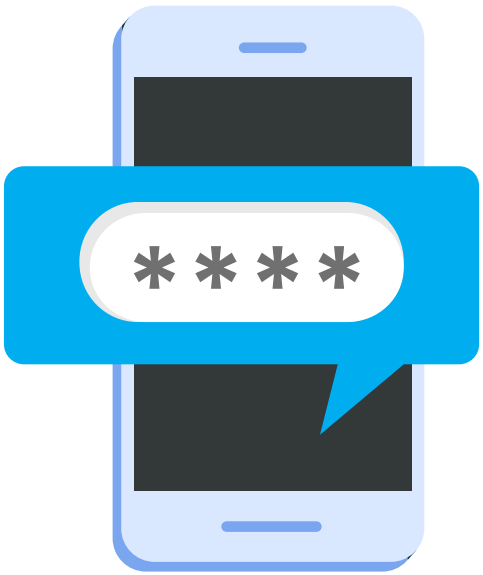
Hoe goed je je bedrijf ook beschermt, er is altijd een kans dat je ten prooi valt aan een cyberaanval of een datalek. Laat je dus niet verrassen. Bedenk nu al wat je zou doen in zo'n situatie. Leg alle stappen vast die jij en je medewerkers moeten nemen. Zo ben je beter voorbereid en houd je gemakkelijker het hoofd koel. Onvoorbereide oplossingen maken alles misschien alleen maar erger.

KIES WATERDICHTE WACHTWOORDEN

Eén kort en eenvoudig wachtwoord voor al je toepassingen. Dat klinkt simpel, maar veilig is het niet. Achterhaalt een hacker dat ene wachtwoord? Dan slaat hij zijn slag: toegang tot ál je accounts. Gebruik dus voor alle toepassingen een ander wachtwoord of een wachtwoordzin. Die is moeilijker te hacken en gemakkelijker te onthouden. De veiligste optie? Meervoudige authenticatie. Dan heb je naast je gebruikersnaam en wachtwoord of -zin nog iets extra's nodig om in te loggen:

- een code die je via sms of e-mail krijgt.
- een bevestiging via de biometrische authenticatiefunctionaliteiten van je mobiele telefoon.

Op die manier maak je het hackers wel erg moeilijk.



Extra tips

1. **Voer minstens een keer per jaar een risicoanalyse uit om eventuele zwakke punten bloot te leggen.**
2. **Leer je medewerkers om bewust om te gaan met e-mails. En vertel hen waar ze terechtkunnen met vragen of twijfels.**
3. **Installeer updates altijd meteen. Windows 10 doet dat automatisch voor jou.**