

Digitale weerbaarheid: Wat kan ik zelf doen?

De digitalisering van de maatschappij in het algemeen en die van het notariaat in het bijzonder gaat steeds verder. Tegelijk neemt de cybercriminaliteit toe. Steeds vaker horen we het cliché: 'Het is niet de vraag of je slachtoffer zal zijn maar wanneer!' Gelukkig kun je zelf veel doen om grote schade te voorkomen: een paar belangrijke tips.

WACHTWOORDEN Feit

Het raden van een lang wachtwoord kost onnoemelijk veel tijd.

Als een wachtwoord bestaat uit cijfers, kleine letters en hoofdletters, dan kost het raden van een wachtwoord van 12 karakters bijna 3.500 keer zoveel tijd als een wachtwoord van 10 karakters (3 weken). Het raden van een wachtwoord van 14 karakters kost zelfs meer dan 13 miljoen keer zoveel tijd!



Tip Kies wachtwoordzinnen die jezelf makkelijk kan onthouden. Dan hoef je ze ook niet periodiek te wijzigen. Let op: uiteraard moet je wel je wachtwoord wijzigen als je vermoedt dat iemand dit weet. Check of jouw wachtwoord is gelekt op haveibeenpwned.com. Grote datalekken van gebruikersnamen en wachtwoorden worden daar geregistreerd.

MULTIFACTORAUTHENTICATIE Feit

Bij 61 procent van de geslaagde hacks wordt gebruikgemaakt van gestolen of geraden wachtwoorden.



Dit was mogelijk omdat er geen multifactorauthenticatie (MFA) via bijvoorbeeld sms of authenticator-app vereist was.



Tip Stel waar mogelijk MFA in voor toegang via het internet tot uw informatie.

Let op: Als je op onverklaarbare momenten het verzoek krijgt om de MFA te bevestigen, wordt mogelijk je account misbruikt. Wijzig dan onmiddellijk je wachtwoord.

PATCHING EN UPDATEN Feit

48 procent tot 56 procent van alle ransomware-aanvallen wordt veroorzaakt doordat aanvallers toegang tot systemen en netwerken krijgen via kwetsbare software.



Tip Investeer in het structureel en tijdig updaten van software op werkplekken, servers en netwerkapparatuur. Dit verkleint de kans op een ransomware-aanval aanzienlijk.

Let op: Installeer niet alleen altijd de updates van het besturingssysteem, maar ook die van de geïnstalleerde applicaties zoals een browser, pdf-reader of tekstverwerker.

CALAMITEITENPLAN Feit

56 procent van de bedrijven wereldwijd heeft geen calamiteitenplan waardoor zij geen idee hadden hoe te handelen bij een calamiteit zoals een geslaagde ransomware-aanval.



Tip Denk al vast na over wat u op kantoor kunt doen als blijkt dat uw computersysteem niet meer toegankelijk is door bijvoorbeeld ransomware.

Let op: Bewaar gegevens van belangrijke contactpersonen (IT-leverancier, cybersecurityverzekering, 06-nummers personeel) in een envelop in de kluis.

