AUTORITEIT
PERSOONSGEGEVENS

5 tips voor zorginstellingen om een datalek te voorkomen

Zorginstellingen kunnen bepaalde maatregelen nemen om de kans op een datalek te verkleinen, of de gevolgen ervan te beperken. Met deze maatregelen kunt u een aantal veel voorkomende typen datalekken voorkomen.

Door menselijke fouten kunnen medische gegevens bij een verkeerde ontvanger terecht komen, bijvoorbeeld door een typefout in het e-mailadres, of door een verkeerde geadresseerde aan te klikken.

- Dit kunt u voorkomen door ervoor te kiezen om de gevoelige gegevens als bijlage op te nemen in het e-mailbericht en deze bijlage te versleutelen met een wachtwoord.
- Dit wachtwoord kunt u vervolgens via een apart kanaal (bijvoorbeeld door te bellen of per SMS) doorgeven aan de ontvanger.
- U kunt zich ook afvragen of e-mail wel het juiste digitale communicatie middel is om dit soort gevoelige gegevens te versturen en bijvoorbeeld overwegen om communicatie via een portaal te organiseren.

Gevoelige dossiers zoals medische dossiers, (jeugd)hulpdossiers, en verslagen over behandeltrajecten worden weleens meegenomen naar huis, bijvoorbeeld in het kader van thuiswerken. Dossiers worden per abuis verloren, vergeten in de trein, of soms zelfs gestolen.

- Voorkom dit door nooit gevoelige papieren zorgdossiers mee naar huis te nemen.
- Scan de dossiers op kantoor en bewaar deze op een beveiligde (versleutelde) harde schijf, USB-stick of in een veilig documentmanagementsysteem binnen het IT-netwerk van uw organisatie. U kunt in het laatstgenoemde geval de dossiers dan thuis raadplegen wanneer u inlogt op de beveiligde netwerkomgeving.

Zorginstellingen slaan soms medische gegevens van patiënten lokaal op draagbare apparatuur, zoals tablets, smartphones, laptops of USB-sticks op. Medewerkers nemen deze gegevensdragers weleens mee naar huis. Met risico's op verlies en diefstal waardoor persoonsgegevens in verkeerde handen kunnen vallen.

- Voorkom dit door geen medische gegevens op te slaan op draagbare apparatuur.
- Maakt u wel gebruik van draagbare apparatuur? Zorg dan dat u deze persoonsgegevens altijd versleuteld opslaat. Zo beperkt u de risico's voor de betrokkenen, wanneer u een draagbaar apparaat verliest of wanneer deze wordt gestolen.

Zorginstellingen, met name ziekenhuizen, zijn vaak doelwit zijn van dit phishing-aanvallen. Daardoor kan een hacker toegang krijgen tot het account van de medewerker. Vaak misbruiken hackers het account vervolgens om nieuwe phishing- of spamberichten te versturen. Dat kan tot nieuwe inbreuken leiden, en/of tot (financiële) schade voor de betrokkenen.

- Verklein de kans op phishing-aanvallen door uw medewerkers bewust te maken van phishing.
- Zorg ervoor dat medewerkers phishing e-mails kunnen herkennen.
- Installer goede firewalls en update deze tijdig, zodat u ongewenste e-mailberichten, zoals spam- en phishing berichten, zoveel mogelijk kunt onderscheppen en blokkeren.

Met name kleinere zorginstellingen en zorgverleners zoals fysiotherapeuten en huisartsen worden regelmatig getroffen door ransomware. Vaak als gevolg van gebrekkige (kennis over) beveiliging. Als gevolg van ransomware kunnen de gegevens op uw systeem in handen komen van hackers, en kunt u permanent of tijdelijk de toegang tot uw gegevens verliezen.

Maatregelen waarmee u het risico op een datalek bijvoorbeeld door ransomware verkleint:

- Installeer software-updates op tijd
- Gebruik geen verouderde (netwerk)protocollen
- Zorg voor gesegmenteerde (gescheiden) computernetwerken en -systemen
- Maak regelmatig back-ups te zodat u altijd beschikking heeft tot de persoonsgegevens, ook wanneer u getroffen wordt door een ransomware-aanval.