

TOOLBOX 47. VEILIG GEBRUIK MAAS IT FACILITEITEN

november 2020

Cyberincidenten kunnen MAAS in het hart raken en gedurende korte of langere tijd verlammen. MAAS is in grote mate afhankelijk van digitale processen. Door de situatie die is ontstaan door het coronavirus, waarbij veel meer via digitale middelen wordt gedaan, is MAAS alleen maar afhankelijker geworden. Aan de slag dus om je digitale weerbaarheid te verhogen! MAAS heeft een aantal huisregels voor het veilig gebruiken van de MAAS IT faciliteiten.

Hoe moet je veilig en betrouwbaar inloggen?

- De MAAS scherm achtergrond is verplicht en mag niet aangepast worden;
- Bewaar je MAAS inloggegevens veilig en deel ze niet met anderen;
- Gebruik je inloggegevens niet voor toepassingen buiten MAAS;
- Maak geen gebruik van wachtwoord beheerapps. Hackers gaan als eerste op zoek naar dit soort apps omdat ze dan meerdere wachtwoorden tegelijk kunnen vergaren;
- Als je het vermoeden hebt dat je inloggegevens uitgelekt zijn, neem dan direct contact op met MAAS Systeembeheer via ICThelpdesk@maas.nl
- Als het uitlekken van inloggegevens toegang geeft tot niet-versleutelde persoonsgegevens betekent dit een inbreuk in verband met persoonsgegevens (datalek). Meld dit direct aan MAAS Systeembeheer via ICThelpdesk@maas.nl

Hoe moet je veilig en betrouwbaar e-mailen?

- Maak op smartphones bij voorkeur gebruik van de Microsoft Outlook app. Dit voorkomt veel mail en kalender problemen;
- Open geen mail bijlagen van een onbekende verzender;
- Klik niet op een link in een mail van een onbekende verzender;
- Installeer geen programma's zonder toestemming van MAAS Systeembeheer;
- Verzending en beantwoording van berichten, geschiedt onder je eigen verantwoordelijkheid;
- Zodra je vermoedt dat bepaalde ontvangen berichten strijdig zijn met wet- en regelgeving, niet van gepaste aard zijn dan wel de integriteit en goede naam van MAAS zouden kunnen schaden, informeer dan direct MAAS Systeembeheer via ICThelpdesk@maas.nl;
- Beperk verzending van vertrouwelijke informatie;
- Als je het vermoeden hebt dat je apparatuur gehackt is, neem dan direct contact op met MAAS Systeembeheer via ICThelpdesk@maas.nl;
- Een cyberaanval waarbij persoonsgegevens zijn buitgemaakt of een besmetting met ransomware waarbij persoonsgegevens ontoegankelijk zijn gemaakt betekent een inbreuk in verband met persoonsgegevens (datalek). Meld dit direct aan MAAS Systeembeheer via ICThelpdesk@maas.nl

Wat zijn de huisregels rond diefstal of verlies?

- Neem maatregelen om diefstal van MAAS apparatuur te voorkomen;
- Als je laptop; verloren of gestolen is, geef dit dan direct door aan Systeembeheer via ICThelpdesk@maas.nl;

- Verlies of diefstal van apparatuur of USB-stick met niet-versleutelde persoonsgegevens betekent een inbreuk in verband met persoonsgegevens (datalek). Meld dit direct aan MAAS Systeembeheer via ICThelpdesk@maas.nl;

Wat verstaat MAAS onder een adequate databaseveiliging?

- MAAS is verantwoordelijk voor de zakelijke data maar ook om juridische redenen dient zakelijke data voor MAAS te allen tijde toegankelijk te zijn;
- Download geen MAAS data op privé computers of computers van derden;
- Maak, zonder voorafgaand overleg met MAAS Systeembeheer, geen zakelijk gebruik van de gratis diensten zoals Google Forms, Whatsapp, WeTransfer, Onedrive of Dropbox;
- Zakelijke data dienen op herkenbare MAAS systemen opgeslagen te worden, zoals het SAP systeem, MAAS fileservers (drive N of H) en in geval van een web interface dient de website herkenbaar te zijn als een MAAS website (MAAS.NL) met een geldig certificaat;
- Op MAAS computers dient zakelijke data bij voorkeur op drive N of H opgeslagen te worden en dus niet op de lokale disk en de desktop, zodat de data op de MAAS fileservers ligt en in de backup meegenomen wordt. Mocht dit niet haalbaar zijn, maak dan regelmatig een kopie naar een MAAS fileserver;
- Het verlies van zakelijke data met persoonsgegevens betekent een inbreuk in verband met persoonsgegevens (datalek). Meld dit direct aan MAAS Systeembeheer via ICThelpdesk@maas.nl

Wat zijn de voorkeur applicaties die je bij MAAS moet gebruiken?

- De voorkeur internet verkenner is Microsoft Edge.
- Microsoft Internet Verkenner 11 is op onze systemen aanwezig voor verouderde websites die niet werken in Microsoft Edge. Voor alle andere Internet verkenners geldt dat de gebruiker zelf verantwoordelijk is voor de installatie van beveiligingsupdates. De meest populaire Internet verkenner (Google Chrome) is een zware belasting voor het geheugen van je systeem;
- De voorkeur voor bestanden mailen is Microsoft Outlook;
- Indien je andere & nieuwe applicaties voor zakelijke data wilt gaan gebruiken, neem dan vooraf en direct contact op met MAAS Systeembeheer via ICThelpdesk@maas.nl

Wat doe je bij een inbreuk in verband met persoonsgegevens (datalek)?

- MAAS is wettelijk verplicht (AVG en UAVG) om elk datalek voor persoonsgegevens te registreren in het MAAS datalek register;
- Wanneer MAAS niet snel genoeg of helemaal niet in actie komt bij een datalek voor persoonsgegevens, gaat MAAS in overtreding. Wanneer de Autoriteit Persoonsgegevens (AP) een tip ontvangt van MAAS klanten of anderen dat MAAS een mogelijk meldplichtig datalek niet bij de AP heeft gemeld, gaan wij in overtreding. Dit zal het vertrouwen in de MAAS organisatie schaden;
- Overige incidenten bij digitale dienstverleners worden door hen gemeld bij het CSIRT (Computer Security Incident Response Team), conform de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni);

Heb je aanvullende vragen over de bovenstaande regels?

Neem dan contact op met MAAS Systeembeheer via ICThelpdesk@maas.nl