Matto Fransen / m.j.fransen@rug.nl

USB-stick gevonden?

Matto Fransen is de nieuwe security manager bij het CIT. Met deze functie probeert de RUG het 'security bewustzijn' bij de gebruikers van de universitaire ICT-voorzieningen te bevorderen.

ICT is ons leven binnen gedrongen en heeft daarin een belangrijke plaats gekregen. Het is daarom noodzakelijk na te denken over de bescherming van onze systemen en de informatie die we daarin hebben opgeslagen.

We kunnen de risico's beperken door bewust te zijn van de gevaren en bewust te handelen. Helaas liggen heel wat gevaren op de loer en moeten we op meer dan alleen de bekende phisingmails alert zijn.

Verleiden

Regelmatig verschijnt berichtgeving waarin aandacht wordt gevraagd voor het bestaan van phisingmail. Via flyers, posters, nieuwsbrieven en tijdschriftartikelen wordt hier aandacht voor gevraagd.

Phisingmails zijn mails die van de universiteit of een andere vertrouwde partij afkomstig lijken te zijn, maar die in werkelijkheid door kwaadwillenden worden verstuurd met als doel in te breken in IT-systemen, bijvoorbeeld door accountgegevens los te troggelen, zoals de inlognaam en het wachtwoord, of bijvoorbeeld om ransomware te verspreiden.

Diverse bewustwordingscampagnes moeten zorgen dat mensen zich minder snel laten verleiden door phisingmails. Helaas zijn dit soort mailtjes niet de enige manier waarop geprobeerd wordt onze IT-systemen te compromitteren.

Supermarktactie

Een variant van phisingmails zijn berichten op bijvoorbeeld Facebook, die wijzen naar webpagina's die heel erg lijken op officiële pagina's. Bijvoorbeeld een nauwelijks van echt te onderscheiden pagina van een online krant of van de website van een supermarkt. Om het beeld van authenticiteit te versterken, wordt soms ook nog onderin commentaar van zogenaamde bezoekers opgenomen, die ook nog eens op elkaar reageren.

De inhoud is een geloofwaardig krantenartikel of een geloofwaardige supermarktactie. In de pagina zijn linkjes verwerkt naar een actiepagina, waar je bijvoorbeeld iets kunt winnen. Het doel is de bezoeker te verleiden allerlei gegevens in te vullen, misschien met een namaak-loginpagina waar de gebruikersnaam en wachtwoord van bijvoorbeeld uw facebookaccount moeten worden ingevuld. Het uiteindelijke doel is hetzelfde als bij de phisingmail, alleen het kanaal via welke het bij de gebruiker komt, is anders.

Het is erg belangrijk om het webadres in de browserbalk te controleren, zeker wanneer een gebruikersnaam of wachtwoord moet worden ingevoerd, of persoonlijke gegevens gevraagd worden. Check in zulke situaties niet alleen het webadres maar ook het 'groene slotje' van de browser.

USB-stick gevonden?

Een andere vorm van cybercrime vindt plaats via een zogenaamde verloren USB-stick. Uit onderzoekt blijkt dat relatief veel mensen geneigd zijn een gevonden stick in de pc te stoppen, bijvoorbeeld om te zien of ze kunnen achterhalen wie de stick verloren heeft. Of uit nieuwsgierigheid, om te zien wat er op staat. Wat doet u wanneer u een USB-stick vindt? Maakt het nog uit of het een ongemerkte stick is, of dat iemand er een

plakkertje met 'foto's strandvakantie' op gedaan heeft? Helaas is het onverstandig een gevonden stick in uw computer te stoppen.

Cybercriminelen proberen altijd zwakheden uit te buiten, of dat nu technische zwakheden in programmatuur zijn, of menselijk gedrag. Zo zijn gevallen bekend, waarbij USB-sticks op een parkeerplaats werden achter gelaten, net alsof iemand er een verloren is. Dit waren echter met malware geïnfecteerde USB-sticks, en wanneer de argeloze vinder deze in zijn of haar werkstation prikt, dan maakt de betreffende malware meteen een backdoor in de pc, waarmee de kwaadwillende ongemerkt op de pc kan binnenkomen, rondkijken en processen kan opstarten.

Gratis stroom

Voor sommige mensen heeft de kans gratis leuke dingetjes te krijgen een onweerstaanbare aantrekkingskracht. Wat doet u, wanneer u bijvoorbeeld op een beurs of conferentie, een gratis USB-stick kunt krijgen? Neemt u die aan, en zo ja, gaat u die dan daadwerkelijk gebruiken? Dit geldt niet alleen voor USB-sticks, maar ook voor allerlei USB-gadgets. Knipperende kerstboompjes, zingende kerstmannetjes, fitness-trackers, het kunnen allemaal apparaatjes zijn die gericht zijn op het ongemerkt binnendringen van uw computer of tablet.

Een andere variant is het aanbieden van gratis stroom voor het opladen van een mobiele telefoon, tablet op laptop. Wie op een congres of in een winkelcentrum een kabeltje van een onbekende in zijn apparaat prikt, loopt heel wat risico's. Wilt u gebruikmaken van zo'n service, doe dat dan alleen om een powerbank op te laden. En die gebruikt u dan weer op zijn beurt om uw smartphone of tablet van stroom te voorzien.

Kwetsbaarheid verminderen

Bescherm u zelf ook tegen de bedreiging van ransomware. Wat gebeurt er wanneer dit zich onverhoopt op uw computer genesteld heeft en al uw bestanden zijn versleuteld? Heeft u dan backups waar u op terug kunt vallen? Op het werk moet u daarom nooit bestanden op de lokale harde schijf zetten, maar altijd op de centrale netwerkopslag (X of Y, of bijvoorbeeld op Unishare).

Hoe is dat op uw laptop? Staan daar bestanden die u eigenlijk niet kunt verliezen? Of thuis op uw computer? Persoonlijke foto's en video's zijn vaak onvervangbaar. Zorg dat u geen slachtoffer wordt van ransomware. Bedenk bij elk bestand wat de impact van het mogelijk verlies van dat bestand is. Is het een bestand dat u niet wilt kwijtraken, zorg dan voor een veilige kopie, die bij een ransomware aanval niet verloren raakt. Wanneer u zo'n kopie op een draagbare USB-schijf maakt, koppel de schijf dan los van de computer, anders levert het geen bescherming tegen ransomware, of bijvoorbeeld een bliksemslag in de buurt.

Verder is het belangrijk de updates altijd te installeren. Deze updates dienen zich zelden op een geschikt moment aan, maar met uitstel van de installatie er van doet u zich zelf geen goed. Updates bevatten meestal niet alleen nieuwe features, maar ook vaak oplossingen van beveiligingsproblemen. Installeer daarom altijd de updates, en liefst zo snel mogelijk. Daarmee vermindert u de kwetsbaarheid, ook voor ransomware.

Blijf alert

Er bestaat een complete wereldwijde industrie rondom de profielen van mensen. Hier gaat erg veel geld in om. Deze industrie richt zich op het verzamelen van gegevens, opbouwen van profielen, en het handelen er in. Iedere keer wanneer u informatie over u zelf achter laat, via bijvoorbeeld de sociale media, dan helpt u deze industrie. Wees daarom voorzichtig en bedenk vooraf, of u bepaalde informatie wel wilt delen en wat op de langere termijn daarvan de consequenties kunnen zijn.

Houd er rekening mee dat de combinatie van uw gebruikersnaam en wachtwoord geld waard is. Bedenk dat uw profiel geld waard is. Blijf alert, wantrouw linkjes in mailtjes en sociale mediaberichten, en controleer altijd op inlogpagina's en op pagina's waar u persoonlijke informatie moet invullen, het webadres in de browserbalk en het groene slotje in de browser.

Geen scrupules

Natuurlijk heeft niet iedereen die gratis USB-sticks of gadgets weggeeft, of een USB-stick verliest of een oplaaddienst voor accu's aanbiedt, daarmee iets slechts in de zin. In de meeste gevallen gaat om een onschuldige actie. Maar helaas leven we in een wereld waarin een gezonde dosis argwaan noodzakelijk is.

Met andermans informatie valt veel geld te verdienen, en er zijn altijd mensen die dat zonder scrupules wel willen proberen. En daarom is het toch verstandig, om niet zomaar die USB-stick, de USB-gadget of dat oplaadkabeltje aan uw apparaat te koppelen. Gevonden sticks kunt u het beste inleveren bij een punt voor gevonden voorwerpen. En wanneer ergens gratis USB-dingetjes uitgedeeld worden, kunt u daar maar beter voor bedanken.