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

OZON 2018:

een grootscheepse cybercrisisoefening

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

Begin oktober deed de RUG mee aan OZON 2018. Dit is een landelijke cybercrisisoefening waar veel Nederlandse universiteiten aan meededen. De website was gehackt, belangrijke data werd versleuteld en vertrouwelijke informatie was gestolen. Tot overmaat van ramp werden we ook nog gechanteerd. De RUG moest betalen, zo niet, dan werd de gestolen vertrouwelijke informatie publiekelijk gemaakt. Althans, dat was het scenario van de oefening.

Malafide server

Om de werkelijkheid zo goed mogelijk na te bootsen, werd gebruik gemaakt van een mediasimulator, waar een storm van Twitter-, Facebook- en persberichten losbarstte. De communicatieafdeling van de RUG draaide op volle toeren om het allemaal bij te benen en te bepalen waar hoe op te reageren.

Ook binnen het CIT stond de druk er goed op. Een phishingmail-aanval werd gebruikt om inloggegevens van RUG-medewerkers te achterhalen, vervolgens werden die gegevens misbruikt om een ransomware-aanval uit te voeren, maar ook om vertrouwelijke informatie te ontsluiten en naar een malafide server door te sturen. Het CERT-RUG (het computer emergency response team van de universiteit) schaalde op en richtte een crisisteam in. Parallel daaraan besloot het topniveau van de organisatie het crisisprotocol te activeren.

Goed bewaard geheim

OZON is een tweejaarlijkse cybercrisisoefening die vanuit SURF georganiseerd wordt. Ook SURF zelf deed aan de oefening mee en bootste intern een grote cybercalamiteit na op de technische omgeving van SURF. De oefening werd ook dit jaar vanuit Utrecht gecoördineerd. Alle oefenleiders van de deelnemende universiteiten kwamen daar bij elkaar en zetten vanaf die locatie de verschillende acties uit, met als doel de druk alsmaar te verhogen en de crisis steeds verder te intensiveren. Aan de oefening ging een maandenlange voorbereiding vooraf, waarbij men goed geheim heeft weten te houden wat er stond te gebeuren. Binnen de universiteit was alleen bekend op welke dagen de oefening plaatsvond, maar verder waren geen gegevens vrijgegeven.

Oefeningen zijn heel belangrijk. Iedereen kent wel de periodieke oefeningen met betrekking tot de brandveiligheid en bijvoorbeeld EHBO. Ook op andere noodsituaties bereidt men zich met behulp van oefeningen voor. Inmiddels zijn we zo afhankelijk van de digitale systemen, dat een cybercalamiteit grote gevolgen voor het functioneren van de organisatie kan hebben en de universiteit onderkent daarom ook het belang van cybercrisisoefeningen.

Realistisch scenario

De RUG deed mee aan OZON 2018 om te oefenen in het omgaan met zo'n grootschalige crisis, en om te zien in hoeverre we op een dergelijke situatie zijn voorbereid. Kloppen de protocollen nog, weet iedereen zijn rol en zijn de interne communicatieplannen voldoende effectief. Dit zijn voorbeelden van elementen die gedurende de oefening werden getest.

Wat tijdens de oefening opviel, was dat iedereen in zijn rol zat en serieus meedeed. Na afloop vertelden verschillende betrokkenen dat het oefenscenario heel realistisch was. Ook werd weer duidelijk hoe intensief het omgaan met grootschalige calamiteiten is.

De deelname van de RUG aan de cybercrisisoefening was een succes. Doordat iedereen serieus deelnam aan de oefening, werd de crisisorganisatie echt getest. De cyberdreigingen werden systematisch aangepakt en de communicatie tussen de crisisorganisatie aan de top van de universiteit, het CERT-crisisteam en de communicatieafdeling kwam goed tot stand. Een oefening om van te leren, en de komende tijd worden een aantal verbeterpunten doorgevoerd, die tijdens de oefening naar voren zijn gekomen.

Gevaar van phishingmail

Wat ook tijdens de oefening weer opnieuw bleek, is dat ingaan op phishingmail een groot risico met zich meebrengt. Dit gaat verder dan alleen de eigen data en het eigen werkstation. Blijf daarom waakzaam en wees voorzichtig met het klikken op linkjes in mailtjes...