Information gällande cyberincidenten

Detta har hänt:

Under morgonen onsdagen den 22 februari uppmärksammades Aon Sweden på att kunder och andra mottagit spammail innehållande skadlig kod. Mailen har varit designade så att de vid första anblick ser ut att vara skickade från en aon-address med traditionellt svenska namn som avsändare och som informerar om att en faktura finns att betala. Avsändarnamnet har varierat men alla meddelanden ser ut att ha skickats från domännamnet @aon.at. Domännamnet tillhör inte och kan inte kontrolleras av Aon. Mailen saknar också helt loggor eller andra attribut som kopplas till Aon.

Detta spammail innehåller ett så kallad ransomware vilket är en typ av skadlig programvara som låser datorns alla filer om man klickar på länken i mailet. För att låsa upp filerna krävs mottagaren på en lösensumma i Bitcoins. Även anställda inom Aon Sweden har nåtts av detta spam.

Detta görs från Aons sida:

Aons lokala och globala IT-team samt Aons cybersäkerhetsgrupp har arbetat aktivt för att snabbt skaffa sig en överblick av omfattningen av denna incident, samt undersöka vilka möjligheter Aon har att förhindra vidare spamutskick.

Aon har kontakt med Austria Online, vilka först identifierades som den mailvärd de ansvariga för attacken använt sig av för att skicka spammet från. Vidare undersökningar av det skadliga mailet tyder på att man använd så kallat ”mailnull” för att dölja den riktiga e-postadressen. @aon.at verkar alltså ha används som ett slags falskt kuvert för utskicket, vilket således innebär att inte heller Austria Online kan råda över situationen.

Aon uppdaterar kontinuerligt anställda, kunder och allmänheten om information som framkommer i takt med undersökningarna.

Vad kan du göra:

Som tidigare informerats uppmanar vi alla att vara vaksamma och att inte öppna epost från domänadressen @aon.at samt att följa sina interna riktlinjer för misstänkt skadlig epost.

Vi har fått frågor gällande spamfilter och normalt kan funktionen i ett spamfilter konfigureras så att den enbart blockerar mail från, i detta fall, aon.at-domänen och inte allt som skickas från aon.se (eller aon.com).

Information about the cyber incident

What's happened:

In the morning of February 22, Aon Sweden was informed that clients and others had received email spam containing malware. The email spam have been designed so as to give the impression of being sent from legitimate Aon addresses, with traditional Swedish sender names, informing recipients that they have an invoice to pay. The sender names vary, but all messages have been sent from the user domain @aon.at. The domain is not owned or controlled by Aon. The emails lack logos and any other Aon attributes.

The email spam contain so called ransomware, which is a type of malicious software that locks all of the computer files by clicking the link in the email. To unlock the files, recipients are prompted to pay ransom in Bitcoins. Aon Sweden employees have also received the email spam.

Action taken:

Aon's local and global IT teams and Aon's Cyber Security Group have been working to quickly get a grasp of the extent of this incident, as well as exploring any opportunities Aon may have to prevent further email spam.

Aon has contacted Austria Online, an Austrian telecom company that was initially identified as the responsible party for the domain that the perpetrators had used to send the spam. Further investigations have however indicated that the perpetrators used so called "mail null" to mask the actual email address. @aon.at appears not to be the actual envelope address, and the use of the address would thus be impossible for Austria Online to impact.

Aon will provide updates to staff, clients and the public as information is made available through the investigations.

What you can do:

As previously informed, we advise that you are cautious and refrain from opening emails from the @aon.at domain address and to follow any applicable company guidelines for suspected malicious email.

We have received questions regarding spam filters. These can normally be configured in such a way that emails are blocked only if they, in this case, come from @aon.at, in order to avoid that all (non-malicious) correspondence from aon.se or aon.com is blocked.