Advance Notification of Off-site E-mail hosting threats

Security Advisory AE-Advisory 16-33 **Criticality** Critical

Issue Discovered On 25 September 2016
Advisory Released On 26 September 2016

Impact

Disclosure of confidential government information.

Mitigation

- It is recommended that government entities host their own e-mail servers or any services inside the country in their own datacenter.

Affected Groups

- Government Entities hosting their servers and services outside the United Arab Emirates.

CVE Reference

N/A

Summary

It has been brought to our attention that some government entities are hosting their email servers or services outside the United Arab Emirates based on numerous reasons. This is a huge threat to the entity itself as different countries have different regulations and privacy laws and these email servers hosted outside the country are not falling under the UAE rules and regulations. According to the UAE's Federal Policy (Law Number 21 for Year 2013, Article Number 4) all federal entities are strictly forbidden from hosting their e-mail servers outside the country by using third party e-mail service providers such as: Gmail, Hotmail, Yahoo…etc. As this could lead to several privacy issues and disclosure of confidential government information. This can create chaos for the entity if their servers and/or services are compromised and confidential information is exposed to the public. This is further explained in the "Threat Details" section below.

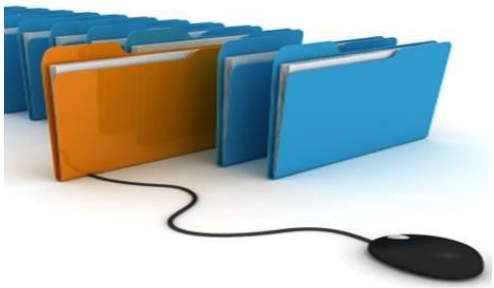
Threat Details

Email is still an important means of communication between the entities. Recently there has been noticed an increasing number of government entities outsourcing their email services to third party e-mail service providers located outside the country like Google, Yahoo...etc. for numerous reasons such as saving operation cost or shortage of staff and so on. However, there are many risks associated with this case, below are the main risks of outsourcing the government mail servers or any other services outside the country:

1. Privacy

Hosting the government email servers outside the country means that you trust the other parties to keep your data private. When the hosting company changes its privacy policy, you can never be certain about the privacy of your data. With your email hosted on servers housed within the entity datacenter or in any datacenter located inside the country, you can control all aspects of its privacy. This includes not only who has administrative access to accounts, and network access to the service, but also physical access to the hardware the service it is running on. In addition to that, these email hosted inside the country will be falling under the UAE laws and regulation.

2. Policies



Hosting the government email servers inside the country gives you full control over policies governing your data, such as the data-retention policy, data-retention policies may be critical aspects, especially as these emails are belonging to the government. Being able to control your policies to retain mail only as long as needed, or for as long as possible may be an important consideration.

Hosting outside the United Arab Emirates can bring a lot of negative impacts to the government entities. For example: Whether it's a website or a mail server, if it has been compromised by attackers, it would be hard to communicate with the hosting company and get information about the attack logs, IP addresses and other critical information off them. This will create a huge issue because the entity will not know anything about the attack details and might not be able to mitigate whatever happened and reduce the risks of being attacked next time. There is also the risk of exposing confidential information exchanged between e-mails by the entity because of the compromise that took place by the attackers. It is believed that many of the government entities are hosting outside because the cost is much lower and some are not aware of what the risks are of doing so. If a mail server is attacked and compromised, even if the hosting company refused to give out the information and the entity decided to go with reporting the case it would be a very long process which includes channels of communications between countries and so on. Therefore, it is recommended to host within the United Arab Emirates whether inside the entity's own infrastructure or using some of the solutions provided in this advisory.

Mitigation

- Host your own e-mail server
- Using any managed services

Other References

http://www.tra.gov.ae/processfile.php?file=20141116162128-legal_references-Cabinet-Resolution-No-21-2013.pdf&l=en

Contact Us

aeCERT
P.O. Box 116688
Dubai, United Arab Emirates
Tel (+971) 4 230 0003
Fax (+971) 4 230 0100
Email info[at]aeCERT.ae

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to aeCERT[at]aeCERT.ae