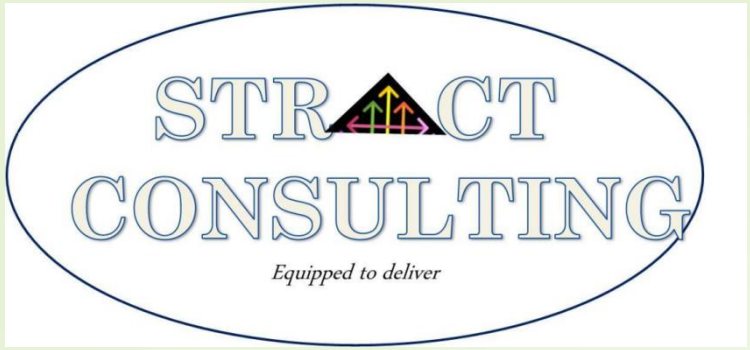

Stract Consulting Limited

Cybersecurity Incidents Review 2016

Stract Consulting | Year in Review

Summary

- 2016 has been year of many cybersecurity incidents and we continue to see various incidents of varying scale. The highlight of 2016 are:
  - Most high profile local attack – Theft of confidential emails from the Ministry of Foreign Affairs
  - Most persistent cybercriminals: Ransomware attackers
  - Biggest data breach: Theft of 1 billion Yahoo Mail accounts
  - Most politically charged breach: Russians interference with the US elections
  - Biggest hack-activist – hacking of WADA's database exposin confidential information on Olympic athletes

Examples

- In this report we highlight a sample of local and internation events that were highly publicized. These include:
  - Theft of emails from the ministry of Foreign affairs in Kenya
  - Defacement of ODMs website
  - Hacking of social media accounts of Kenyan Celebrities
  - Russian interference with the US elections through hacking of the Democratic emails
  - Theft of Yahoo accounts
  - Breach of the WADA database to expose athletes using banned substances 'legally'

What we have learnt

- There are several lessons that we have learnt from these breaches. Key among them are:
  - Social engineering continues to be the most used attack method by adversaries such as spear phishing of emails
  - Attackers are interested in confidential information that can be used to blackmail service providers
  - State sponsored attacks continue to rise and can be used to carry out regime changes
  - While the controls around the social media providers continue to improve, hackers are targeting celebrities and high profile persons using social media.

STRACT CONSULTING
Equipped to deliver

Stract Consulting | Year in Review | Local

REPUBLIC OF KENYA

MINISTRY OF FOREIGN AFFAIRS

Incident

- Ministry of Foreign affairs theft of 1TB of data

Date:

- April 2016

Attack Vector:

- Anonymous

Vulnerability

- Phishing

Summary:

- Hackers were able to send phishing emails to staff a the Ministry of Foreign affairs. Those who clicked on the phishing emails, were ended up providing passwords to the hackers. The hackers were able to steal confidential and non-confidential PDF and Word files from the ministry server including email conversations, security related communication, international trade agreements and letters discussing the security situation in (South) Sudan where government forces are fighting the Sudan People's Liberation Army (SPLA).

What we learnt

- Social engineering contributed largely to this incident. This can be eradicated through **employee information security awareness** workshops as well as through **email filtering tools** that can spot phishing emails.

STRACT CONSULTING
Equipped to deliver

Stract Consulting | Year in Review | Local

Incident

- Defacing of ODMs website

Date:

- June 2016

Attack Vector:

- Dark_Ghost

Vulnerability

- Not publicized – Either vulnerabilities on the webserver or hijacking of the admin password

Summary:

- In June the website of Orange Democractic Movement (ODM), the second largest political party in Kenya was defaced by a hacker who goes by the name Dark_Ghost as per Zone-H records. In addition to the defacement the site was re-directing users to adult sites.

What we learnt

- Ensure that your web server is running the current version and is **fully patched**. Ensure that admin passwords are well **secured**.

STRACT CONSULTING
Equipped to deliver

Stract Consulting | Year in Review | Local

Incident

- Social Media Accounts of Celebrities

Date:

- Throughout 2016

Attack Vector:

- Various

Vulnerability

- Password theft, social engineering

Summary:

- Social media accounts of various celebrities were hacked in 2016. This included:
  - The Twitter account of Radio Personality Maina Kageni
  - The Facebook account of Aswani who plays for AFC leopard
  - Musician Bahati's Instagram account

What we learnt

- Passwords are not enough security for social media accounts. Enable **multi-factor authentication** which are provided by the social media companies that can involve some one time verification codes sent through the phone among others.

STRACT CONSULTING
Equipped to deliver

Stract Consulting | Year in Review | International

Incident

- US Elections interference

Date:

- July 2016

Attack Vector:

- Suspect – Russian Government, Fancy Bear, Cozy Bear

Vulnerability

- Email hacks

Summary:

- Emails of the Democratic National Committee (DNC) were hacked and released by WikiLeaks. The emails showed that it favored Hillary Clinton over her competitors. Political pundits have claimed that this could have been the reason Hillary Clinton lost the presidency to Donald Trump. The CIA and other US intelligent agencies claimed that the hacks were carried out through the support of the Russian Government

What we learnt

- Elections hacks illustrates that regime changes can now be carried out through cyber attacks. As Kenya gears for the election in 2016, with a lot of automation on both the sides of the political divide as well as on the IEBC it important to assess the risk of cyber security as well have measures to **monitor, detect, respond and contain** cyber attacks.

STRACT CONSULTING
Equipped to deliver

Stract Consulting | Year in Review | International

Incident

- Yahoo 1 Billion Accounts theft

Date:

- September 2016

Attack Vector:

- State sponsored actor

Vulnerability

- Advanced Persistent Threat (APT)

Summary:

- Yahoo announced that as a result of 2014 breach the account information of its customers totalling 1 billion accounts had been stolen. The account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords and, in some cases, encrypted or unencrypted security questions and answers,

What we learnt

- For end users, still using their yahoo accounts, it meant they have to change their passwords, security question and answer as well as enable two factor authentication. For service providers handling customer data it means that such information must be stored more securely and should be encrypted while at storage or in transit.

STRACT CONSULTING
Equipped to deliver

Stract Consulting | Year in Review | International

Incident

- World Anti-Doping Agency (WADA) hack of Therapeutic Use Exemptions files for athletes

Date:

- September 2016

Hacker:

- Fancy Bear – Russian hacking group

Attack Vector

- Spear Phishing

Summary:

- Hot on the heels of the Olympics where a large number of Russian athletes were banned because of doping, the Russian hacking group Fancy bear hacked into WADA's database and exposed a number of athletes who had been allowed to use banned substances for therapeutic purposes. Luckily there was no Kenyan athlete who was exposed.

What we learnt

- There is an increase in hack-activist who would go at great lengths to target organizations to illustrate any wrong doing. It illustrates that every organization must take security of any confidential information it has seriously. Well resourced hacking groups like Fancy bear will stop at noting to hack into computer systems.

STRACT CONSULTING
Equipped to deliver