Cyber Attacks

John Finch, Plymouth City Council

PLYMOUTH
CITY COUNCIL

Notification

- 29 email addresses and passwords were found in a password dump on the website Virus Total.
- Staff passwords were changed in case they had been used for corporate network access.

Initial analysis

- The email addresses were all from the same department
- Some had a commonality about the password, which gave an indication of the website they had been used on.
- The website was externally hosted and developed.
- It stored data supplied by people external to the Council.

Additional information requested

- The supplier was asked to switch off the website and supply the following:
  - A copy of the data stored by the website.
  - All available log files for the website.
  - Any available traffic statistics supplied by the hosting company.
- Supplier also asked to analyse the website code for any vulnerabilities.
- A full copy of the password dump file was also obtained.

Detailed analysis

- An impact assessment was conducted on the data in the website
- The dump file was compared to the database
- The data in the database directly correlated to email addresses in the dump file
  - The scope of the breach was much wider than just 29 addresses
- The log files showed SQL injection attacks and other unusual activity

Escalation

- SIRO was notified
- CERT-UK were contacted
  - Advice was provided to contact law enforcement
- Report made on Action fraud
- SW Cyber-crime team (Zephyr) got in contact
  - All relevant information supplied
- ICO was notified

Remediation

- Communications plan was initiated
- Those affected were contacted by letter
- Helpline implemented for people to contact for advice

After effects

- There was a very low response from those affected
- Details made the local press, however quickly fell down the news rankings
  - No comments on the article
- The ICO took no further action
- Investigation took several months
- Manual process used instead of website for medium term

Findings

- Attackers were from foreign jurisdiction
  - Took great steps to obfuscate their identity
- Main target was email addresses and passwords
  - These have a potential value on dark web
    - Rest of data did not
- The data was taken after the website had become obsolete
- Website did not have expected security built in at development stage
- Log file retention and traffic analysis was insufficient

Is this a one-off?

- Dump files are appearing on the Internet with increasing frequency
- Data breaches have been happening for decades, some of this data is now being circulated on a wider basis
- There is a lot of vulnerable historical data still accessible on the internet
  - Some may have been dormant and unmanaged for years
  - Data will exist in internet archives
- Websites are still being developed insecurely
- Complexity of modern interactive websites can introduce vulnerabilities from 3rd parties

What you can do

- Impact assess all websites that process your data
- Insist on security development and accreditation on all websites
- Sign up to CISP
  - Notification of similar dumps has already taken place
- Monitor websites like Virus Total, Pastebin for data containing your domain
- Have a response plan in place

Response plan

- Analyse the data very quickly
- Identify any commonality between email addresses
- Identify any website affected
  - If internal or commissioned – Switch it off and secure all log files
  - If external – notify the website
- Obtain original data from website if possible
- Assess scope of data affected
- Assess impact of data breach

Response plan

- Implement escalation appropriate for impact
- Implement communications plan
- Engage with CERT and law enforcement
- Ensure all relevant data can be supplied
  - Scope of breach
  - Impact assessment
  - log files
- Identify lessons learnt and implement.

Nationally?

- Website accreditation as standard
  - Tested for vulnerabilities
  - Standards for monitoring
  - Compulsory breach notification
- Local regions can share intelligence on breaches found
- Standardise process for notification, management and remediation
- National bodies can monitor and notify all affected by breach
  - Recent dump files found had multiple government domains
- Simplify Reporting process

Cyber Attacks

John Finch, Plymouth City Council

PLYMOUTH
CITY COUNCIL