Attackers Constantly Threaten the Survival of Organisations, but there is a New Shark in the Water: Carcharodon Carcharias

Moderator Europa Universalis

Bob Duncan
University of Aberdeen
11th June 2018
Attackers Constantly Threaten the Survival of Organisations, but there is a New Shark in the Water: Carcharodon Carcharias Moderator Europa Universalis

- Introduction
- The Cloud Forensic Problem
- GDPR Background and Related Work
- Minimum Requirements for GDPR Compliance
- Is it Possible to Achieve GDPR without Addressing the Cloud Forensic Problem?
- Sensible Mitigation Strategies
- Proposed Pilot Study, Aims and Limitations
- Conclusion
Attackers Constantly Threaten the Survival of Organisations, but there is a New Shark in the Water: Carcharodon Carcharias
Moderator Europa Universalis

Introduction

- Companies are continually subject to cyber attack
  - Under GDPR, companies must report breaches within 72 hours
- All cyber security is challenging, but Cloud presents special challenges
  - GDPR fines can be punitive
  - What difference will Brexit make?

Cyber Science 2018, Pioneering Research & Innovation in Cyber Situational Awareness, Glasgow, Scotland, 11th – 12th June 2018
Attackers Constantly Threaten the Survival of Organisations, but there is a New Shark in the Water: Carcharodon Carcharias Moderator Europa Universalis

- The Cloud Forensic Problem
  - What is it?
  - Why is it a problem?
  - GDPR Compliance
Attackers Constantly Threaten the Survival of Organisations, but there is a New Shark in the Water: Carcharodon Carcharias

Moderator Europa Universalis

- GDPR Background and Related Work
  - Early work on the GDPR was mostly covered by legal academics
    - A few Computer Scientists got involved
  - Comparison with Previous Legislation and Regulation
Attacks by Cyber Threats Continuously Put Organisations at Risk, but a New Threat Emerges: Carcharodon Carcharias

The Minimum Requirements for Compliance

- Provide a Right of Access
- Provide the Right to Erasure
- Provide Privacy by Design
- When breached, report the breach within 72 hours
- Notify the Data Subject if adverse impact is identified
- What extra steps do you need to do for cloud?

Cyber Science 2018, Pioneering Research & Innovation in Cyber Situational Awareness, Glasgow, Scotland, 11th – 12th June 2018
Attackers Constantly Threaten the Survival of Organisations, but there is a New Shark in the Water: Carcharodon Carcharias Moderator Europa Universalis

- The Minimum Requirements for Compliance
  - What extra steps do you need to do for cloud?
    - Encrypt ALL PII data locally
    - Keep encryption and de-encryption keys off the cloud
    - Ensure a full audit trail is maintained off cloud
  - Full forensic records of all users who use the database backend must be collected and stored offsite

Cyber Science 2018, Pioneering Research & Innovation in Cyber Situational Awareness, Glasgow, Scotland, 11th – 12th June 2018
Attackers Constantly Threaten the Survival of Organisations, but there is a New Shark in the Water: Carcharodon Carcharias Moderator Europa Universalis

- Can You Achieve Compliance without Addressing the Cloud Forensic Problem?

- A great many companies often cannot tell they have been breached

- The average time between breach and discovery had been reducing year on year until the change in the GDPR reporting

- The longer an intruder remains undetected, the more damage they can cause

Cyber Science 2018, Pioneering Research & Innovation in Cyber Situational Awareness, Glasgow, Scotland, 11th – 12th June 2018
Sensible Suggestions to Mitigate the Potential Impact of the GDPR

- Encrypt all Personally Identifiable Information locally
- Keep all encryption and de-cryption keys off cloud
- Maintain a full audit trail of the entire database off cloud
- Maintain full forensic records off cloud
Attackers Constantly Threaten the Survival of Organisations, but there is a New Shark in the Water: Carcharodon Carcharias Moderator Europa Universalis

- Proposed Pilot Study
  - HP Microserver to run a cloud environment
  - Raspberry Pi devices configured as clients
  - Raspberry Pi devices configured as attackers
  - A private router with 24 port network switch
  - All running hardwired LAN connections

Cyber Science 2018, Pioneering Research & Innovation in Cyber Situational Awareness, Glasgow, Scotland, 11th – 12th June 2018
Attackeds Constantly Threaten the Survival of Organisations, but there is a New Shark in the Water: Carcharodon Carcharias Moderator Europa Universalis

- Proposed Pilot Study Goals
  - Teach students how to configure secure cloud instances
    - Teach students how attacks can be perpetrated
  - Have some attacks perpetrated by guest penetration testers
  - Test how well our proposed framework can resist attack

Cyber Science 2018, Pioneering Research & Innovation in Cyber Situational Awareness, Glasgow, Scotland, 11th – 12th June 2018
Attacksers Constantly Threaten the Survival of Organisations, but there is a New Shark in the Water: Carcharodon Carcharias Moderator Europa Universalis

- Limitations and Discussion
- University of Aberdeen
  - 11th June 2018
Attackers Constantly Threaten the Survival of Organisations, but there is a New Shark in the Water: Carcharodon Carcharias Moderator Europa Universalis

- Conclusion

- GDPR will present a serious wake up call
  - We have identified the key requirements for compliance
  - We have proposed a simple means to mitigate the risk of fines
    - Our approach should permit faster breach discovery

Cyber Science 2018, Pioneering Research & Innovation in Cyber Situational Awareness, Glasgow, Scotland, 11th – 12th June 2018
Attackers Constantly Threaten the Survival of Organisations, but there is a New Shark in the Water: *Carcharodon Carcharias*

Moderator Europa Universalis

- Any Questions?