Bournemouth University

BSc (Hons) Cyber Security Management

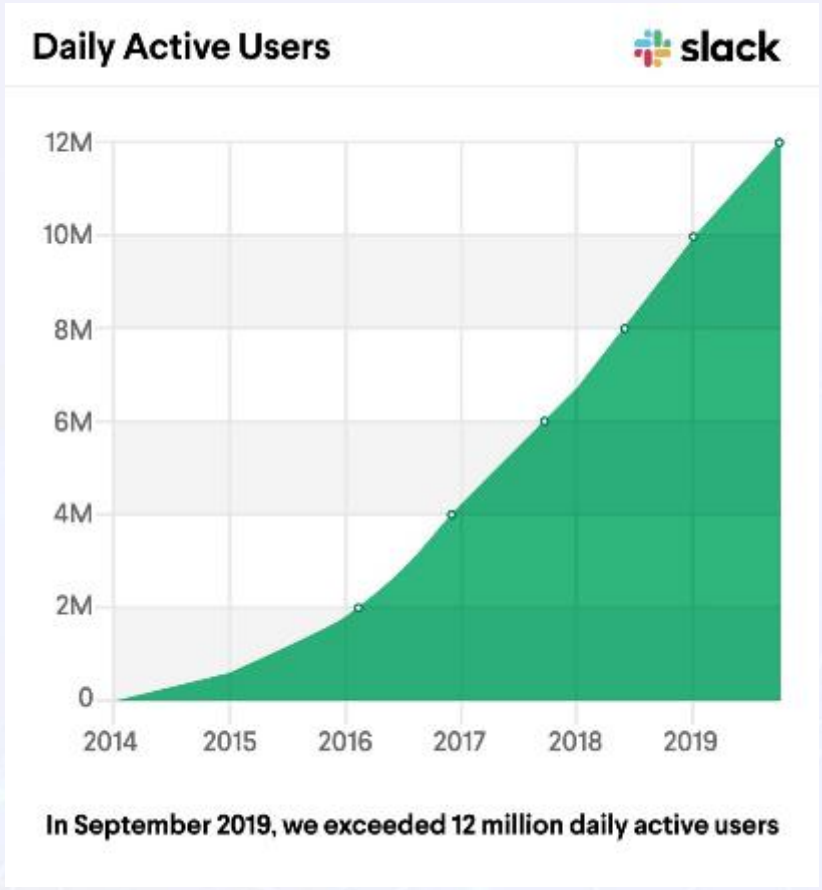
Luke Wood

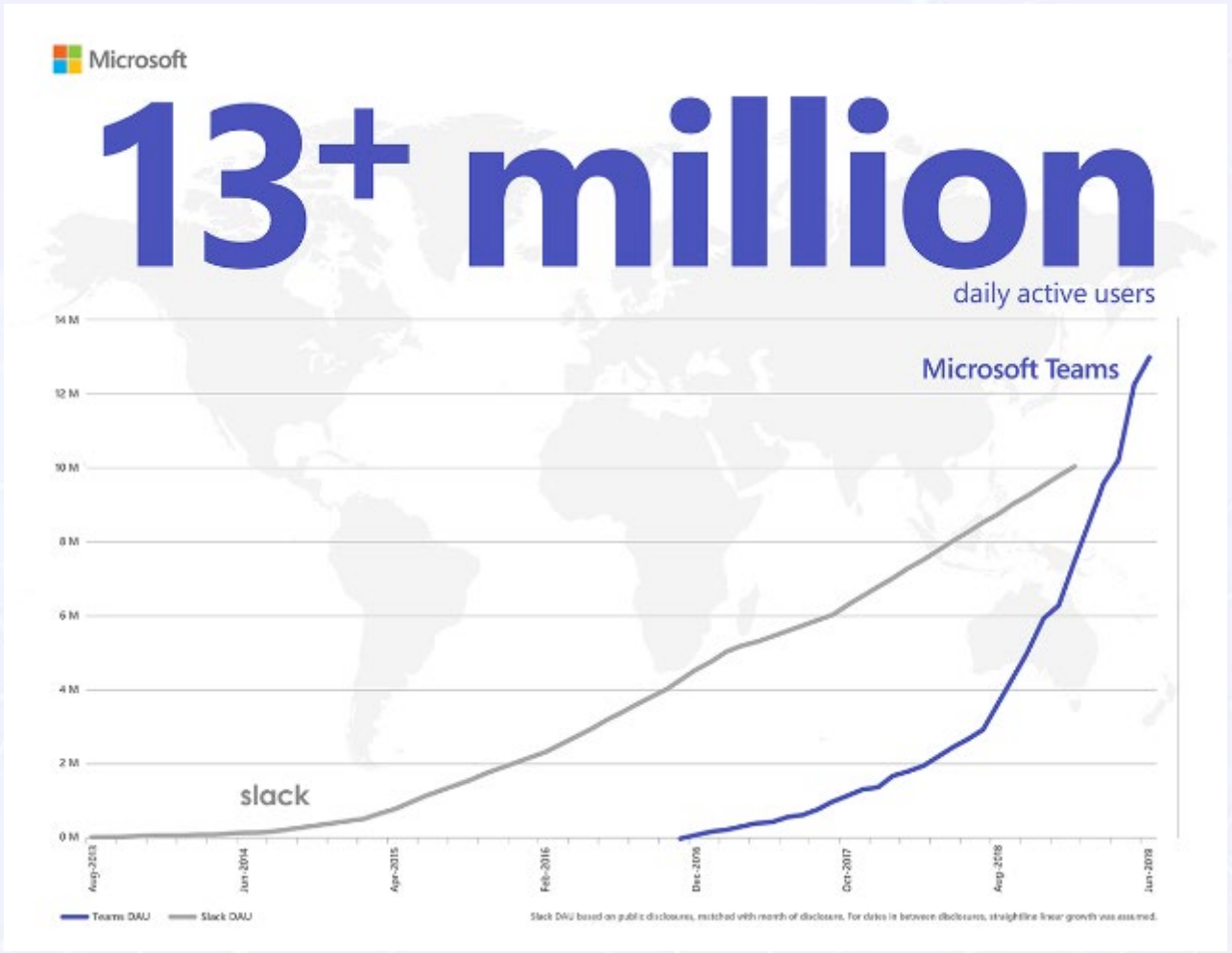
An information risk management system for instant messaging applications

Outline

1. Context
2. Problem
3. Background
4. Objectives
5. Approach
6. Solution
7. Testing
8. Discussion
9. Conclusion

Adoption Rate





Bournemouth University

Beware of the GIF: Account Takeover Vulnerability in Microsoft Teams

Slack resets tens of thousands of passwords following 2015 data breach

It's estimated around 100,000 users are affected.

EDITORS' PICK | 21,259 views | May 2, 2020, 07:03am EDT

Beware This New Microsoft Teams Password Hacking Threat To 75 Million Users

Slack fixes vulnerability exploitable for session hijacking, account takeovers

Cisco Webex phishing attack wants to steal your logins

May 8, 2020 | Abnormal Security | Abnormal Security

Problem

- A growing dependency and adoption rate for instant messaging (IM) applications has made IM an attractive attack vector for performing cyber-attacks and delivering malware proving the need for an IM risk management system.

Background

- IM is an ever changing threat landscape with a serious lacking in a publicly available IM risk management system.
- 75% of organisations will use workspace collaboration tools by 2023 compared to 45% in 2019 – Gartner (Gotta and Preset 2019)

IM Risks

- Phishing.
- Malware.
- Account takeovers.
- Vulnerabilities.
- Human error.
- Process risks.

Objectives

1. Assess the current state of the security risks posed by using IM applications within businesses.
2. Evaluate existing security solutions.
3. Obtain specifications and requirements.
4. Design and/or build the system.
5. Test and evaluate the system.
6. Refine the system based on feedback received.

Approach

- Research existing IM risk management systems.
- Analyse those systems or similar technologies for inspiration.
- Gather requirements.
- Design/build system.
- Test and evaluate system.

Requirements

- The system must record details of risks, their controls, and priorities.
- The system must record risk treatments and resource requirements.
- The system must record details of incidents and lesson learned.
- The system should track accountability for risks, controls, and treatments.
- The system should allow for progress checks.
- The system must provide a dictionary of terms.
- The system could show the status of IM applications.
- The system must show various threat feeds for IM applications.
- The system must produce errors into an error log.
- Any changes made to the system must be logged in a change log.
- The system should be accessible from a multitude of devices, i.e. workstations or work phones.
- The system should have a latency of no less than 3 seconds to display information.
- The system must be easily maintainable.

Solution

- Publicly available IM risk management system.
- Showcasing status feeds, threat feeds page, analysis of vulnerabilities, and security controls along with a PESTLE analysis.
- Risk assessment of IM.
- See here for a demo of the system.

Testing

- Blackbox and Whitebox testing.
- Independent testing.
- Knowledge experts.

Discussion

- New tools have been used.
- Calling APIs – biggest challenge.
- Done differently – incorporate more applications, more advanced features.
- Future work – mobile IM applications, integration into SOCs and knowledge experts.

Conclusion

- This project provides a basis in which to aid discussions around the adoption and implementation of IM applications for businesses. IM applications and their weaknesses are a continuously growing landscape as have been discussed in depth throughout this project.

Bournemouth University

Thank You