DevTech Security Audit and Security Recommendations

CONTINUOUS ASSESSMENT

Gordon Reynolds

1 Contents

2 OBJECTIVE

This continuous assessment presents you with a Scenario and Specification using a fictitious company called DevTech. You are then required to submit a solution in response to the given scenario and specification. Your solution will be submitted in the form of a Report (submitted as a PDF via Moodle).

The Continuous Assessment requires you to:

- Propose how you would execute a security audit for DevTech.
- Outline key policies that DevTech should implement.
- Directly address the issues raised in the CA Scenario and Specification

You should clearly outline your reasons for any suggestions made with regards to the above requirements.

3 MARKING SCHEME

The marking scheme for this continuous assessment is broken down as follows (Table 1):

Deliverable	***Mark (x / 100%)***	***Details***
General Formatting	5%	Marks awarded for the general format of the report. This includes the use of Headings, Paragraphs, Tables … etc.
Report structure	5%	Marks awarded for the general structure of the report. This includes Sections, Sub-Sections … etc.
Logical Flow and Report Narrative	20%	Marks awarded for the general flow of the narrative. One section should lead to the next section, different material should be introduced in a logical manner … etc.
Main Body Content	60%	Marks awarded for the content of the main body. Keys areas include i) Conducting a Security Audit ii) Recommending Security Policies and iii) Addressing specific concerns/issues at DevTech.
Referencing	10%	Marks awarded for the use of referencing, this includes table and diagram referencing.

Table 1: Table outlining the Assessment's Marking Scheme

4 DELIVERABLES

This Continuous Assessment requires you to submit a Report via Moodle in PDF format. The report will contain information and details such as (but not limited to):

i. Title Page
ii. Table of Contents
iii. Summary
iv. Overview
v. Suggestions in relation to a security audit
vi. Suggestions in relation to security policies
vii. Suggestions in relation to specific issues
viii. Conclusion
ix. Referencing

4.1 SUBMISSION DETAILS

Submission Format: The report should be saved as a PDF file and named with your Student Number.

Submission Method: The report is to be submitted via Moodle at the Continuous Assessment section using the CA-Submission tool.

5 CA Scenario and Specification

DevTech is a successful start-up company that was founded by four collage friends that has grown from 4 employees to 38 employees. It is expected that DevTech will continue to grow and the founders are expecting staffing levels to pass 70 employees in the next 18 months.

The founders/directors of DevTech have been concerned about security and as a result, you have been hired as their first Security Officer.

During your first week with DevTech, you have met with the founders/directors and various other staff. During this time, you have discussed, observed and noted the following:

1. DevTech is renting a serviced building that is shared with three other companies. Their office space is alarmed, locked by key and has no other form of security.
2. The general organisational structure of DevTech is outlined in Figure 1

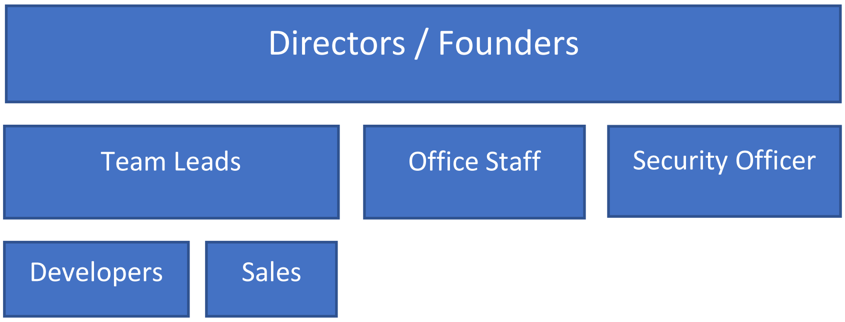

Figure 1: Overview of DevTech's Organisational Structure

3. Their computer hardware consists of:
    a. Mainly laptops
    b. Some desktops
    c. Several servers
    d. Printers
4. Each user manages their own Computer. As a result,
    a. Software installations vary from PC to PC
    b. Each PC is in a different state regarding updates
    c. Each user is an Administrator on their PC
    d. Users install software as required
    e. Anti-virus is not generally up-to-date
    f. Encryption in generally not used, with exception to the Directors.
    g. Laptops and desktops are not backed-up.
    h. Some files are stored locally on the PC and some files are stored on a server.
    i. The Operating System of choice is MS Windows 10. These are connected using four MS Workgroups.
5. There is a general absence of official IT documentation, this includes:
    a. Operational Guides,
    b. Company IT Policies,
    c. Company IT Processes
    d. Other General IT Documentation.

6. Regarding their network environment,
    a. Their network is based on a single IP subnet (192.168.10.0/24). This subnet is used for company laptops, servers, printers, wifi and guest wifi.
    b. The network hardware consists of three 16-port network switches daisy chained together and a pre-2013 firewall. In general, the firewall is not managed.
    c. DevTech have six servers. These are kept under desks near the users. Each server is backed up weekly using an external HDD that is left directly connected to the server.
    d. All users have administrative privileges to the servers for file storage and file retrieval.
7. Office Operations
    a. Laptops are generally not locked away (when left in the office)
    b. Employees regularly bring their laptops home.
    c. Employees tend to have lunch at their desk.
8. The Directors have several concerns,
    a. Being hit badly by Malware
    b. Data lose
    c. A concern that IT security will interfere with productivity and/or system usability

5.1 YOUR DELIVERABLES

The directors have asked you to prepare a plan for the next 12 months. This plan is to include:

- A Security Audit
- Review and Implementation of Policies
- Additional Recommendations

Submit this plan as a report, outlining how you would conduct a security audit (and why), recommend policies that DevTech should implement (and why) and outline any other security issues with mitigation suggestions that you might have.