Access Control and Authorization

Who Can Do What?

CyberSecure Fleming Group Project Winter 2023

Prof Mamdouh Mina, Computer Security & Investigation

Scope

EXAMPLE OF SCOPE STATEMENT - The following policy applies to all employees, contractors, visitors, and recognized affiliates of Fuzzy Bunny LTD. It will be applicable to all devices and systems that have either/or a general or administrative account with Fuzzy Bunny LTD

Account Types and Allowances

General Accounts – Administered by Fuzzy Bunny LTD. No admin rights given. Will have access only to what is necessary to perform the employees function. Any requests for further access must go through the Information Technology section. Email checking and limited web surfing will be allowed.

Administrative Accounts – These accounts are to be used for admin duties only. All users with an admin account must also have a general account to perform their normal day to day activities. This will be the accounts that are able to change software, perform software updates, and disable software as needed/prescribed. Only employees in the Information Technology section will be given this type of account.

Identity & Access Management

Some organizations have a point person(s) who manage who can have bigger access. In other places, it may work better if a group is responsible for this. Ultimately, this will come down to the size of the company. Either way is, in principle, approved by CyberSecure. If a centralized system is not feasible, then this section requires a writeup detailing that it is not applicable.

Enforcement

EXAMPLE OF SCOPE STATEMENT – The responsible party to create and maintain user accounts at Fuzzy Bunny LTD is the Information Technology section. These accounts be given out based on the needs of the company, and on the work the employee is expected to perform. Team leaders, supervisors, and managers are required to verify their employees need the accounts they have, subject to future auditing.

Additional Concerns for Certification

NON-IT EMPLOYEES WITH ADMINISTRATIVE RIGHTS. It is possible that an employee who does not work in your organizations IT department might need higher level access. These occurrences should be rare, temporary, and must be accompanied by an explanation of why it is necessary for that person to have higher access. "Just because", "it's always been this way", and similar arguments will no be looked upon favorably.

ACCOUNT MAINTENANCE. This section is where the company will explain their process of creating, maintaining, and deleting accounts. A regular audit of accounts is a necessity, as it will keep the IT department up to date on what accounts they should have. This will help weed out accounts that should no longer be usable, as well as keep attack accounts at bay.