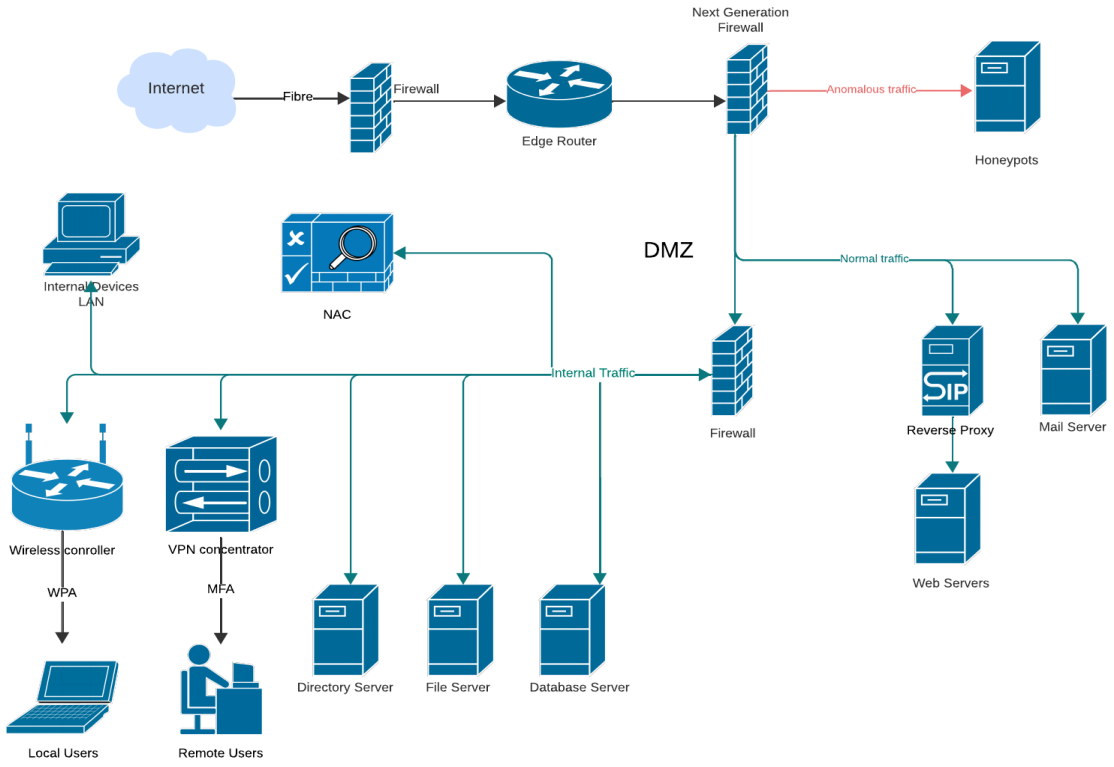
Secure a Network - Lab1

Task 1: Secure Network Diagram

I used my Networking assignments and looked at several architectures on google. This video in particular helped a lot.

Arrows indicate how information is allowed to enter the system. In reality information can flow in all directions given the right authorizations.



First we have the edge router and Next Generation Fire Wall (NGFW) provide the first line of defense against external threats. We divide the network into multiple VLANs to isolate different types of devices and data. This segmentation limits the potential spread of malware and helps contain security breaches. Suspicious clients are sent into a honeypot to track and study them and avoid actual breaches.

Public-facing servers are placed in a Demilitarized Zone (DMZ), separated from the internal network. This configuration protects internal resources from direct external access. This is where the mail server and webserver is placed. We use a reverse proxy that appears to the attacker to be an ordinary web server, but acts as an intermediary forwarding requests to one or more web servers.

In the internal devices (connected via LAN) are separated by an internal firewall, WPA3 Enterprise encryption and separate SSIDs for employees and guests provide strong protection for wireless communications. The VPN concentrator allows secure remote access for employees, using SSL VPN with multi-factor authentication to ensure only authorized users can connect. There are also server farms with servers like Directory, Database and File server all connected and can be accessed after authorization from the internal firewall.

Network Access Control (NAC) authentication ensures that only authorized devices can connect to the network, reducing the risk of rogue devices.

There is ofcourse other methods which will need to be put into a realistic system like Redundancy and Encryption (such as SSL). My goal was to just give a basic idea of the architecture itself.

Task 2: Recent Security Event Article

Summary

I had read about iD tech camps data breach a year ago and it was quite interesting to me. Nearly 1 million user records were exposed, including 415,000 unique email addresses, along with names, birth dates, and plaintext passwords. What's particularly concerning to me is that iD Tech, a company providing tech and coding courses for kids, failed to acknowledge this breach for weeks.

Why the event arose

In my assessment, this breach likely stemmed from a combination of inadequate security measures, delayed detection, and insufficient monitoring. The fact that passwords were stored in plaintext is a glaring red flag to me indicating weak security practices.

What could have been done different prior to the event arising

I believe iD Tech could have mitigated this incident by implementing

1) stronger data protection measures (using hashing)
2) conducting regular security audits (redteam internal servers)

Broader issues

This event raises several critical issues in my mind. I'm particularly concerned about the protection of children's data in digital environments and the apparent lack of corporate transparency. It's clear to me that we need stricter enforcement of data protection laws, especially when it comes to businesses handling children's data.

Potential responses

If I were advising on responses to this breach, I'd recommend that affected individuals immediately change their passwords and monitor their accounts for any suspicious activity. For policymakers, I'd suggest strengthening data protection laws, particularly those related to children's data, and implementing stricter penalties for delayed breach disclosures.