A logo for a college

Description automatically generated

A close up of a logo

Description automatically generated

COSC 1104 – Assignment 2

Angela Jonyl Reyes

100989583

Part 1: Identify the Problem

1. **Cyber Breach Risk Score**

* Data breaches vary in severity depending on factors such as the number of individuals affected or the type of data exposed (e.g., financial information, social security numbers). Organizations need a way to evaluate and prioritize breaches based on their potential impact.

1. **Breach Data Incident Notification**

* The problem this script solves is the manual effort and delay in monitoring breach notifications published on the Maine Office of the Attorney General's website. Specifically, it addresses:

1. Manual Monitoring is Inefficient:

* Without automation, someone must regularly visit the website, locate the table, and sift through the data to identify breaches reported the previous day.

1. Risk of Missing Critical Breach Updates:

* Important breach reports might be missed if no one checks the site daily or if updates are delayed.

1. Time-Sensitive Nature of Breach Information:

* Knowing about breaches promptly allows organizations to act quickly, such as adjusting their security posture, informing affected parties, or mitigating damage.

1. No Default Notification System:

* The Maine AG website does not provide automated alerts to admins or stakeholders, making manual effort the only option.

Part 2: Solution – Breach Data Incident Notification

*https://github.com/angelajonyl/assignment2*

1. Automates Data Collection:
   * The script fetches data daily without manual intervention.
   * It filters the information to show only breaches reported the previous day, streamlining the process.
2. Provides Proactive Notifications:
   * Send emails with the affected organization name and the date the breach was reported, ensuring the admin is alerted promptly.
   * Includes the source link for verification and further action.
3. Scales Well:
   * It can be adapted to include more filters, monitor multiple sites, or send notifications to multiple recipients.

Part 3: Reflection

* What was the most challenging aspect of solving this problem?  
  The most challenging part of solving this problem was configuring the email-sending functionality. Using an app password for the email account was necessary due to modern email providers' stricter security protocols. Setting up the app password and ensuring that the email wasn’t flagged as spam required careful configuration of the SMTP server and credentials. Additionally, ensuring that the script fetched the correct data consistently from the Maine AG website reinforced the importance of accurate HTML parsing and robust error handling.
* Is there something you would still like to add to this, or something it makes you want to try next?

I would like the email to include a direct link for each breach report so the admin can conveniently open the reports for further details. This would save time and provide a seamless way to verify the data. Second, I’d like to enhance the script to cover breach reports from all U.S. states. This would involve researching and integrating data from other attorney general websites or security repositories that track breaches nationally. Additionally, I initially wanted to cover breach incidents from Canada. While researching, I realized finding breach report websites for Canada was difficult. I chose Maine Attorney General website because it provides a structured table and complete details of each breach incident. It would be beneficial if Canada had a centralized system or a similar website to make such information accessible. If such a system becomes available, I would love to adapt the script for Canadian data.

* How did you test your completed product? How confident are you that it works reliably?

I tested the email-sending feature by using a test email account to ensure the notifications were sent and received successfully. This included verifying the formatting of the email and checking if it avoided spam filters. And to verify that it fetched the correct breach data where it limits to reports that were reported a day ago, I ran the script multiple times on different days.

A screenshot of a computer

Description automatically generated

* What resources did you use to learn about the libraries (or any other new features) you used?
  + Python Email and SMTP Documentation - <https://mailtrap.io/blog/python-send-email/>
  + Datetime and Pytz
    - <https://docs.python.org/3/library/datetime.html>
    - <https://pypi.org/project/pytz/>
  + Smtplib and Email Libraries
    - <https://realpython.com/python-send-email/>
    - <https://stackoverflow.com/questions/64505/sending-mail-from-python-using-smtp>
  + BeautifulSoup (bs4) - https://tedboy.github.io/bs4\_doc/