Information Security Management Model

Company description

Mission statement: “To share and create moments with food around the world”

Web Applications: Food Mood (app/social media), Website version/ desktop-accessible

Servers: Web Servers, Database Servers, Application Servers

Departments: Creative & Design, Data & Analytics, Infrastructure, Software engineering, Management, and business strategies

Routers and switches: Cisco CCIE package

Remote access: Global!

Wireless communication: Wireless WAN

Firewall: SonicWall

DMZ: Dual/back-to-back

Current information security risks & threats

Social Engineering: Being a social media platform, social engineering is typically one of the biggest threats to the user base. Often, how the strategy plays out, is a bot usually tries and convinces you to become friends or even a real person pretending to be likable towards you.

They then try to get you to give them personal information about yourself or send you links to other sites or applications that can then make you vulnerable. When events like this occur, users lose trust and start to feel unsafe while using the application. They may feel forced to delete their account and probably won't create a new account. This happens to everyone but most know how to combat it. This is still a huge threat due to not everyone knowing how to handle a social engineering attack.

Phishing Attacks: Phishing is one if not the biggest threat all companies have to face on a daily basis. A phishing attack can happen to anyone and on either side of the network. Developers can easily fall for the same tricks that users do but formatted a little differently. A hacker might want control of a dev account to gain personal information on users on a major scale, they then would sell that information at wholesale. A user could suffer from an attack which could once again lead to information being stolen, or finances lost. How this is prevented by limiting the number of bot accounts and developing a system that prevents these attacks and a warning system as well.

System-specific plan on how to protect property: Intellectual property is constantly attempted to get stolen. This is our plan for how to prevent this. The first step is we are registering all copyrights trademarks and patents that directly come or relate to our application Food Mood. This includes the IPs, domain names, and the creative work that is produced as well. Our important logos and quotes are in the process of receiving a trademark as well. We have also already registered as a business to protect our identity as well.

To ensure nothing important leaves the business walls, we've created confidentiality contracts including non-disclosure and licensing contacts for our employees and partners that are working closely with us. Security measures have also been instated. We have a team that has set up a VPN for us to work on as well as WIFI-protected access. Nothing confidential leaves our established network.

Security Model/Access Control Mechanisms: The access control mechanism food mood will be using whilst in this state of the company is Role-Based Access control (RBCA). The reason this mechanism works best for our company is that we are a technological social media application. There are going to be levels of work and information that not everyone needs to see or know about. There will be personal information on locations people roam and they use while they sign up for the application. It is important that this is stored and only accessed by those who are trusted. There will also be information on upcoming updates and ideas within the company that will help it grow. If this information is leaked by an untrusted source, we are risking possible setbacks or competitors getting ahead. In terms of our security model, we are going to primarily work on the NIST cybersecurity model. This system runs through 5 core steps: identity, protect, detect, respond, and recover. We believe in a food mood, if this is the strategy we use to protect ourselves, we will be ahead of most attacks that will come.

Roles of personnel:

Chief executive officer (Jesse Doe): Manages company's overall operations including delegating and directing agendas, driving prophet, and managing organizational structure.

Chief Information Security Officer (Mary Goose): Responsible for developing and implementing a security program. This includes procedures and policies that will protect the company's enterprise.

Information Technology Director (Joe Green): Runs the technology group within the organization. Ensures IT operations run smoothly and also ensures improvement in the IT process.

Marketing Manager (Joy Brown): Organize marketing campaigns that raise awareness and generate demand and use the application

Finance Manager (Kelly Andrews): perform data analysis and give advice to senior managers on profit-maximizing ideas.

Human Resource Manager (Josh Myers): Direct administrative functions within the company. Oversees interviewing recruiting and hiring of new staff. Consults with top executives on strategic planning.

End users: The public