prensenting for Sam’s Scoops

Threat Landscape Report for Sam’s Scoops

Explaining the threat landscape

Presented by : Sarah Monica Bossongo

November 11, 2024

PROJECT DESCRIPTION

Introduction: Sam's Scoops, a small ice cream business, is expanding its presence online. While this opens up new opportunities for growth, it also exposes the company to various online threats. This report identifies three common online threats that could impact the business, explains the risks associated with each threat, and suggests preventative measures to protect the company from potential cyberattacks.

THE TOPICS I WILL COVER INCLUDE:

- Identify three online threats and explain how each threat is caused.
- Highlight the potential dangers associated with each threat that I have identified.
- Prescribe some preventative methods that I can employ for Sam’s Scoops.

CASE STUDY

The staff at Sam's Scoops are excellent ice cream makers and make a product that is much loved in their seaside community; however, they know little about good online practices. My task is to gather information on the dos and don'ts of online actions and then share my findings with the team. To be more specific, I'll identify three vulnerabilities, and for each one, I'll describe the risk it brings, the type of attack that a cybercriminal might use to exploit it, and a mitigation technique that can be used to reduce risk and improve safety

THREAT NUMBER ONE: PHISHING ATTACKS

[Vulnerability]: Employee email used for business communication
Phishing attacks often target individuals who use email for business communications. Attackers send fraudulent emails that appear to come from a trusted source, like a vendor or a customer, to steal sensitive information like passwords or financial details.

[**Risk**]: Data theft and fraud
If an employee falls victim to a phishing attack, the attacker could gain access to sensitive business information, such as financial records, customer data, or even login credentials to business accounts. This could lead to identity theft, fraud, and financial loss.

[Attack]: Phishing email
Phishing emails are designed to trick employees into clicking a malicious link or downloading an infected attachment. The attacker may impersonate a known supplier or partner, convincing the employee to provide login details or transfer money.

[**Mitigation]: Employee training and email filtering**
To reduce the risk of phishing, employees should be trained to recognize suspicious emails, such as those with strange sender addresses, poor grammar, or urgent requests. Additionally, implementing email filtering systems that flag suspicious emails can prevent many phishing attempts from reaching employees.

THREAT NUMBER TWO: MALWARE AND RANSOMWARE

Vulnerability: Outdated software or lack of security updates
When business systems (such as point-of-sale systems or customer databases) are not regularly updated, they become vulnerable to malware and ransomware attacks. Cybercriminals exploit outdated software to install malicious programs that can cause damage or hold data for ransom.

Risk: **Data loss or service disruption**
Malware can disrupt business operations, damage or delete data, and even render critical systems inoperable. In the case of ransomware, attackers may demand payment to unlock the company's data, leading to financial loss and potential damage to the company's reputation

Attack: Malware , Ransomware
Malware can be designed to perform any number of ill effects on a system once executed. It is a blanket term that can encompass theft of information, disruption of services, or application of ransomware. Injecting it into a system by unsuspectingly clicking on a link can be very harmful.

Ransomware encrypts important files and demands payment (usually in cryptocurrency) to restore access. The attack can spread quickly across the network, affecting servers, databases, and point-of-sale systems, halting business operations

Mitigation: Regular software updates and backup systems
Sam's Scoops should ensure all software, including operating systems and applications, is kept up to date with the latest security patches. They should also implement a robust backup system to keep copies of important data in case of a ransomware attack, allowing the company to restore lost information without paying a ransom

THREAT NUMBER THREE: WEAK PASSWORDS AND UNAUTHORIZED ACCESS

Vulnerability: Weak or reused passwords
Weak passwords (like "123456" or "password") or the reuse of passwords across multiple accounts can make it easy for attackers to gain access to sensitive business systems. If a password is easily guessed or found in a data breach, unauthorized users can log in and access private business information

Risk: Unauthorized access to business systems
If an attacker gains access to the company's accounts (such as online banking, social media accounts, or employee portals), they can steal sensitive data, conduct fraudulent activities, or disrupt business operations.

Attack: Brute force attack
Attackers can use automated tools to guess passwords through brute force, trying common combinations or stolen password lists. If passwords are weak or reused, attackers may successfully gain access to business systems and sensitive data.

Mitigation: Strong password policies and multi-factor authentication (MFA)
To reduce the risk of unauthorized access, Sam's Scoops should implement a strong password policy that requires complex, unique passwords for all business accounts. Additionally, multi-factor authentication (MFA) should be used wherever possible, adding an extra layer of security by requiring both a password and another verification method (such as a text message code)