

Kudler fine foods it security report and presentation – top threats

[Law](#), [Security](#)



Kudler Fine Foods IT Security Report and Presentation - Top Threats Team B has been commissioned to examine the Kudler Fine Foods' (KFF), frequent shopper, CustomerLoyaltyProgram that is currently in development. The team has also been asked to direct the system development team to ensure the system is established securely so that it properly protects company data and customer information throughout all stages of the system development process. In week 2, the team will examine the Customer Loyalty Program for vulnerabilities in different areas of the system. The study will define the possible threats that exist to the security of the organization's and the customers' data and information, the potential vulnerabilities each threat may exploit, and area of the system affected by the threats. Additionally, a summary of the most critical threats to Kudler's Customer Loyalty Program will be provided. The following table presents the possible threats, the potential vulnerabilities each threat may exploit, and area of the system effected by the threats: Area of Systems

Threat

Potential Vulnerability

Networks

Unauthorized access

Unsecured equipment room

Confidentiality breach

E-mail that doesn't employ scanning of messages

Denial of Service

Lack of inside firewall can lead to worm spread

Natural

Disaster

Potential issues from lack of redundancy

Sniffing

Network infiltration via wireless access point

Workstations

Unauthorized access

Patches not current

Sniffing

Old software versions

Natural

Disaster

Firewall not active

Servers

Unauthorized access

Patches not current

Sniffing

Old software versions

Natural

Disaster

Firewall not active

Employees

Social Engineering

Training not current

Corruption

Unhappy

Malicious behavior

poor work ethic

Data

Corruption

Non secured

Deletion

Unencrypted data

Software

Corruption

Non-secured

Deletion

Software that does not employee authorized user access

Building

Tailgating

Front door that doesn't have employee security guard

Unauthorized access

Compromised key card access

Of the possible threats to Kudler Fine Foods' Customer Loyalty Program there are two critical threats discovered during our assessment that warrants Kudler's immediate attention. The first of these threats is Social Engineering. Social Engineering according to Social-Engineer. org (2013), is " the act of influencing a person to accomplish goalsthat may or may not be in the ' target's' best interest. This may include obtaining information, gaining access, or getting the target to take certain action." The employees

themselves are the area of the system affected by this threat. Social Engineering exploits their naivety. General lack of experience in recognizing this type of attack is a major reason for its success. Education on what Social Engineering is and how to recognize attacks coupled with company policies written, put into place, and enforced to prevent individuals from divulging or even having access to certain information no matter the scenario is the recommended course of action.

Next is Denial of Service. According to Conklin, White, Williams, Davis, and Cothren (2012), a Denial of Service (DoS) attack is an attack intended to disrupt a system or service from operating normally. The attacker will attempt, through means of crashing the system, closing out a logged on session, or overwhelming a machine with multiple requests that causes the machine to freeze up or as stated crash. Kudler's Customer Loyalty Program information could be affected because the program that accesses customer information could be made unavailable by such a DoS attack.

This could cause events such as slow terminal responses, systems going offline while updating customer files, and causing system reboots to return to normal operation. This type of attack exploits the weakness of either not having a firewall running in the terminal or server background or a poorly set up firewall allowing too many network requests to be handled by the system. Kudler's IT department should be aware of this and conduct a system check to ensure that the firewall allows requests from only internal or authorized external sources.

As requested by Kudler Fine Foods, Team B has conducted an examination of the Customer Loyalty Program concerning the possible threats and vulnerabilities to their system. A table presenting these threats and vulnerabilities as well as the areas of the system affected has been made available for review. In addition, a summary of the top two critical threats that must be addressed by Kudler Fine Foods has been provided.