**Case Study: Azumer Water**

Azumer Water is a non-governmental organization (NGO) that provides clean drinking water to urban communities in the southwestern United States that have been affected by natural or manmade disasters. The organization is a part of the Federal Emergency Management Agency’s (FEMA) emergency relief efforts. With a vision of “Help communities restore livelihoods,” and a motto of “Clean water heals a community faster in a disaster,” the organization aims to deliver sufficient supplies of bottled drinking water to urban communities within 24 hours of the initial impact.

The organization employs 10 full-time personnel who focus on managing the logistics of water transport and the resources that support the delivery of clean water to the affected urban areas. To accomplish its mission, the organization relies exclusively on regional volunteers who deliver services in the field. The company currently has 1,073 volunteers who live in the southwestern United States and who are trained to deliver pallets of bottled water from regional centers for distribution to individuals.

Information about the volunteers is kept in a database located on a local machine within Azumer Water’s main office in League City, Texas. The database houses the following information for each volunteer:

* basic contact information
* background checks
* training records
* engagement details
* access to regional storage facilities
* last 4 digits of social security number for identity verification

The organization does not keep backup copies of the database, but some employees occasionally make copies on USB drives when they need to complete work tasks in their home offices.

The organization provides its employees with email accounts that use the domain @azumerwater.org. Volunteers use their personal email addresses for communication with the volunteer coordinator, John Smith, who works in the main office. John maintains the volunteer database to which no volunteers have access. Other full-time employees are provisioned access to the database to back up the coordinator outside his regular work hours. Urgent communication during a disaster relief effort is carried out using cell phones or instant messaging. All full-time employees work and coordinate the volunteers in the field from the main office.

The CEO of Azumer Water, Maria Rodriguez, has contracted an IT company, Pruhart Tech, to provide IT services and to maintain the infrastructure of Azumer Water, which includes a web server, an email server, and a database server that reside on the network in the main office on a Linux platform. Most of the applications that are used are open-source.

The company runs open-source database, e-mail, and web servers. The domain of the company assigned by ICANN (Internet Corporation for Assigned Names and Numbers) is azumerwater.org.

Pruhart Tech implemented an enterprise firewall solution between the main office network and ReadyNet, the company’s ISP (Internet Service Provider), but its configuration has been deferred.

Employees can access the network via desktop computers that are available in the main office or by using their personal devices. The main office uses the Wired Equivalent Privacy (WEP) Protocol to connect to its wireless network. When training at the main office, volunteers access the Internet via the wireless network.

Pruhart Tech’s contact at Azumer Water is Maria, who has been exercising a reactive approach to keeping the infrastructure safe. Since no major incident has occurred in the past, Pruhart Tech has not had the opportunity to perform a vulnerability assessment of the infrastructure and proactively mitigate or resolve risks, despite frequent recommendations. Maria, however, is aware that the network is vulnerable but thinks that attacks are unlikely.

Passwords are not required to be changed, and some employees have been using the same access credentials since joining the organization. Although the employee handbook includes a policy on acceptable use and password maintenance, these policies have never been enforced and have not been updated in years. The employee handbook also states the organization’s security goal to maintain the confidentiality, integrity, and accessibility of the volunteer data.

Elecktores, a hacktivist group that advocates for emergency relief everywhere, not just urban areas, has been publicly attacking the limited mission of Azumer Water. As of late, it has been planning a cyber campaign to discourage Azumer Water’s volunteers from participating in relief efforts. Elecktores has already been involved in malicious activities to deliberately cancel the delivery of ordered bottled water from the regional warehouses.

On a Friday afternoon, John received the following email:

From: [water@watersupp1y.int](mailto:water@watersupp1y.int)

Subject: Exclusive offer on water pallets

Dear John,

We have a special on water pallets for $10 a pallet. The offer expires in two days. Act immediately! Make your order at www.watersupp1y.int.

Sincerely,

Stacey

When John read the email, he was busy updating volunteer addresses in the database and he carelessly clicked on the link in the email and landed on a non-existent web page. He made a note to research the offer when he starts his new work week on Monday, as it appeared appealing and cost-saving.

Saturday morning, volunteers started receiving the following email:

From: d0nate@azurewater.int

Subject: Crises happen all the time – Donate now!

Dear volunteer,

Every day in the news you hear of our presence in the field wherever disasters happen. To support our efforts in providing clean water to the communities in need, please click here to donate.

Thank you,

John Smith

Upon clicking on the link in the email, the recipients were presented with a web form to donate to the cause by selecting an amount to be deducted from their credit card. This is a practice that the organization has not used in the past, so some volunteers were confused. Several of them immediately reacted by sending John angry emails.

It is Monday morning, and this is your first day as a new employee of Azumer Water in the role of information security officer. This is a grant-funded position by FEMA, and in your role, you are expected to elevate the overall security posture of the organization by identifying the risks associated to the organization and recommending solutions to remedy the current situation impacting Azumer.

John arrives in the office and meets with you and Maria, who is showing you around the facilities, including the server room. John goes to his desk and, within minutes, he notifies you and Maria that he cannot find the volunteer database, and that he has received 71 emails from angry volunteers.