CASE STUDY

Protecting Critical Assets Against Disasters

BlastWave
www.blastwave.io

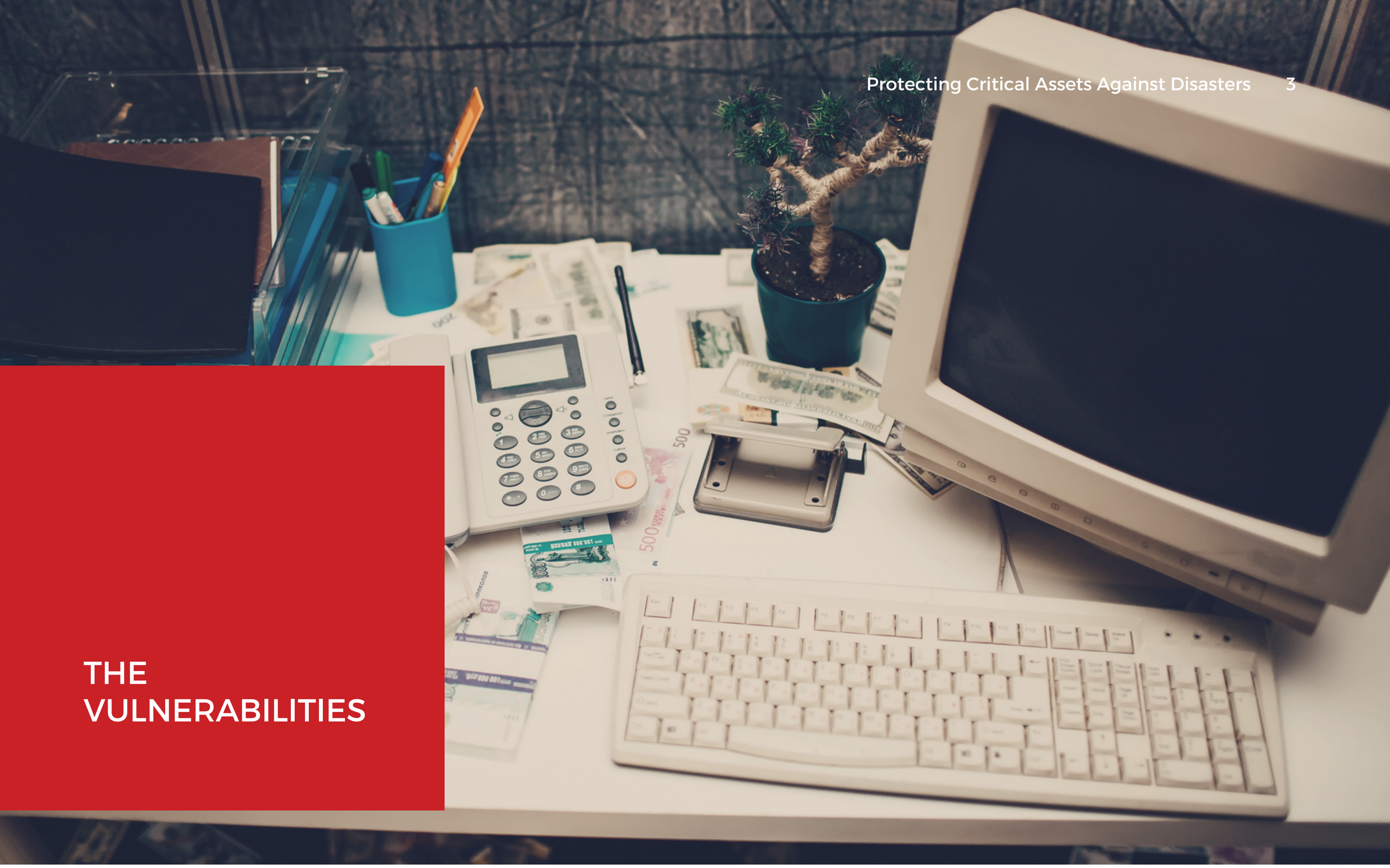
THE POTENTIAL DANGERS

When researching cyber security options and network protection, many CEOs and CISOs are focused on preventing data breaches and leaks. In the summer of 2020, the head of Research and Development of a leading refrigerated and frozen food logistics company learned of an inadvertent security breach via an IT professional's VPN after the pandemic had driven employees to work from home.

The head of R&D recognized how vital it was to secure the network and to protect their company's critical asset—hundreds of football-field-sized refrigerated and frozen facilities utilizing ammonia-based processes for cooling. In large cooling systems, like those, ammonia is commonly used because of its physical properties. In addition, it breaks down quickly in the environment, minimizing potential environmental impact. However, ammonia, if not managed correctly, can be fatal if inhaled, and under compression and high temperatures, as in refrigeration, it can break down into hydrogen and nitrogen dioxide, which are extremely explosive and toxic. These facts make it essential to protect such systems from unintentional and intentional cybersecurity threats.

During the time of the breach, the largest non-nuclear explosion in history, coming from an ammonia plant in Beirut, expedited the company's needs to better protect its critical assets. That single explosion caused numerous fatalities and impacted countless lives costing $15 billion in damages.

Beirut was not a result of terrorism or a security data breach, but understanding the potential risks to a company and the surrounding community was vital in disaster prevention. This recognition, paired with a recent data breach, led the company to search for an alternative to VPN that could enable secure remote access across converged IT and OT environments.



THE VULNERABILITIES

The refrigeration facilities used a combination of legacy Windows 1998 and Team Viewer to manage several systems at their warehouses remotely.

The PC is running industrial control software that controls a refrigeration system.

The PC is running an out-of-date Windows operating system that doesn't have current security patching and is, therefore, a security vulnerability.

Its network interface was a potential attack vector for hackers.

The company tested our BlastShield™ solution, the first all-in-one SDP patented solution that combines infrastructure cloaking and passwordless multi-factor authentication (MFA) for identity-based secure remote network access for organizations that adopted a zero-trust security model. BlastShield enables organizations to hide on-premise and cloud workloads from outsiders and insider threats, concealing an organization's infrastructure from cyberattacks through software-defined microsegmentation without modifications to existing network fabric and hardware. After two months of extensive testing without a single outage, they asked for a version of BlastShield™ that could be run on an Android tablet. BlastWave's engineering team promised to deliver that version in a month and was able to provide a tested version in four days.

THE PROOF OF CONCEPT

The testing plan for the protection of a refrigeration controller PC:

TEST 1 - Invisibility
Secure the PCs behind the BlastShield Software running on commodity x86 hardware. Then, run an IP scan to show that unauthorized access shows no visibility to outsiders or insiders who have access to the corporate network.

TEST 2 - Policy Creation
Create Policy Group with PCs and add the endpoints to demonstrate the ease of use for policy creation within the BlastShield Orchestrator.

TEST 3 - Authorized Access
Install BlastShield clients and demonstrate access to authorized assets. Confirm via IP Scan

TEST 4 - Micro-Segmentation
Add and remove assets to demonstrate how micro-segmentation can be achieved. Confirm that items have been removed by IP scan showing invisibility.

TEST 5 - Air Gapping
Demonstrate via IP Scanning how the OT assets are protected against East-West lateral movement on the IT network

TEST 6 - Resilience
Demonstrate how Peer to Peer meshing provides endpoint connectivity with no bottlenecks. Confirm by providing latency checks on the network traffic.

TEST 7 - Overlay Network
Demonstrate protected assets operating as a secure software overlay network.

THE RESULTS

The client continued using the platform with the new tablet client for three more months until they were convinced that BlastShield should be used as a critical component in their security strategy.

BlastShield now protects the PC behind a Gateway and renders it invisible and isolated from potential attackers while at the same time allowing authorized users to connect to the PC for monitoring and control purposes remotely. Additionally, BlastShield is able to protect systems that either haven't been patched or legacy systems that are unsupported and can't be patched.

"BlastShield truly works. In test after test, I was unsuccessful at circumventing its passwordless MFA login for remote access as well as break outside the software-defined microsegmentation to pivot around inside the network."

- Alissa Knight, Former CISO, Recovering Hacker