Our vulnerability to cyberattacks and personal countermeasures you should take

The United States is fighting a losing war, and the American people are kept in the dark about it. No, I'm not talking about the War on Drugs since we lost this one a while ago. The war I'm referring to is a new type of war taking place in the cyber arena, cyber warfare.

With rapid advancements in technology, the value of information has skyrocketed, and our infrastructure is constantly under attack by both amateur and professional hackers. While some hackers are stealing personal information, such as credit card data and medical records, others are targeting critical infrastructure with the sole purpose of making life difficult for all of us.

There are certain vulnerabilities that have a direct impact on our daily lives, and hospitals and utilities are the targets that have lately seen an increase in cyber attacks. While you don't play a role in protecting such infrastructures, it's your duty to become informed about the weaknesses of our critical infrastructures and prepare for their failure so that you and yours will always be safe.

While, for example, it's impossible to completely protect against an attack on the entire electrical grid, it's

essential to plan and prepare countermeasures to mitigate the immediate impact and aid recovery.

The most vulnerable infrastructure, the electrical grid

In 2013, it was reported that a group of Iranian hackers had attempted to penetrate the computer systems of a U.S. power company. The group, known as “APT33” or “Elfin,” targeted a number of organizations in the energy and aerospace sectors, including a US-based company that provides control system technology for industrial applications, including the power sector.

According to reports, the hackers used a variety of techniques to gain access to the targeted systems, including phishing emails, watering hole attacks, and malware-laden attachments. The specific aim of the attack was not clear, but it was believed to be part of a broader campaign by the Iranian government to gather intelligence and potentially disrupt critical infrastructure.

The following year, the U.S. Department of Homeland Security (DHS) issued a report warning that Russian hackers had targeted the U.S. power grid, among other critical infrastructure sectors. The report stated that the hackers had gained access to the control systems of several U.S. energy companies and had the capability to cause significant damage to the grid.

The DHS report did not provide details on the specific methods used by the Iranian hackers, but it did state that the group had been active since at least 2011 and had targeted a range of sectors beyond energy, including water, aviation, and government agencies.

And with the recent war in Ukraine, it seems that such attacks

continue to evolve and become more sophisticated, and the risk of a successful attack on critical infrastructure remains a concern for governments worldwide.

General impact

The power grid’s outdated infrastructure is vulnerable to exploitation, but some providers are adopting an “air gap” approach to disconnect from the Internet. Nevertheless, once breached, these systems are often vulnerable to permanent damage.

For the general public, a successful attack on the power grid can have disastrous consequences, and we have seen before how a power grid failure can cost people their lives.

In February 2021, Texas experienced a severe winter storm that resulted in widespread power outages across the state. The state’s power grid, operated by the Electric Reliability Council of Texas (ERCOT), was not able to keep up with the high demand for electricity caused by the extreme weather conditions, which led to rolling blackouts and, in some cases, prolonged power outages.

According to reports, at least 111 people died as a result of the storm and power outages, with many of the deaths occurring in the Houston area. The majority of the deaths were due to hypothermia, but others were attributed to traffic accidents, fires, and other causes related to the crisis.

What can you do?

If you are one of us like-minded preparedness individuals, you should know by now that there are certain steps you can take to prepare for such an attack for both short-term and long-term scenarios.

For a short-term scenario, a backup power source is crucial, and the number one choice for most Americans is generators.

While these are effective, they are also quite expensive, require fuel, and may not be feasible for all. If you have limited resources or space, an alternative power option would be to stock up on backup batteries or power banks.

For a short-term solution, you need to invest in a system that can generate electricity from renewable sources, such as solar or wind energy. Here it all depends on your location and the resources you can use. Residential solar panels are becoming increasingly affordable and can provide a decent amount of electricity if stored in moderately sized battery banks.

The best option is to have all of the above, but unfortunately, many people may not take these steps to prepare. We constantly see this on T.V., and when an event leaves people without power, the news channels show people waiting in lines to get their hands on a generator.

The water supply

We take water for granted in this country, and we cover our water needs with a simple turn of the tap, but few people actually know what's going on behind the scenes and what it takes to deliver potable water to people's homes. While the infrastructure itself is not in the best of shape and it requires constant maintenance, it seems that those responsible for your water supply also need to deal with cyber-attacks and the threat they pose.

For example, here are some of the incidents that were made public:

In 2016, the city of Dallas, Texas, experienced a cyberattack on its water supply system. The attack, which was reportedly carried out by hackers based in Iran, targeted a system that controlled the city's water pumps. The attack did not result in any significant damage or disruptions to the water supply, but it raised concerns about the vulnerability of such

critical infrastructure and how easily it can be overpowered by cyberattacks.

Three years later in 2019, a cyberattack on a water treatment plant in Oldsmar, Florida, resulted in an attempted poisoning of the water supply. The attack, which was carried out by a hacker who gained access to the plant's computer system via remote access software, increased the levels of sodium hydroxide (lye) in the water supply to potentially dangerous levels. Fortunately, the attack was detected and stopped before any harm was done, but it highlighted the risks of cyberattacks on water supplies.

In 2021, a water treatment plant in Ellsworth, Maine, was hit by a ransomware attack. This coordinated attack disrupted the plant's operations and prevented staff from accessing the computer systems that control the water treatment process. Again, while there was no immediate harm to the water supply, the attack underscored the vulnerability of critical infrastructure to cyber threats.

General impact

The hacks on the water treatment plants expose the vast extent of vulnerabilities that exist. This critical infrastructure still holds better than the power grid, but there is no guarantee this situation can go on for long.

It goes without saying that in a survival situation, regardless of the environment you find yourself in, water becomes your number one priority. We can't live for more than a few days without water, and we must always make sure our need for water is covered. While people will figure out how to procure water if the outage lasts for less than a week, the situation will become desperate if the tap stays dry for more than a week.

There are already regions in this country dealing with severe

drought where the population is “encouraged” to save water, and for these regions, a cyberattack crippling the water utilities will have dire consequences on their daily lives. The government will have to intervene to provide water to the people, and such a scenario is a logistical nightmare.

What can you do?

As preppers, we already have our stocks of food and water, but the general public doesn’t seem to be too concerned when it comes to water shortages. Storing water is the first thing people can do, and while this task may be straightforward, in reality, the situation is more complex.

Having extra drinking water may not be enough since water will also be needed for your sanitation task and waste disposal. In today’s modern world, the absence of a functioning toilet can be a significant problem for most Americans, and few of them know what to do when their toilets stop working.

Storing water, as said before, is a complex task since water is both heavy and bulky, and you need to have enough storage space to cover the water needs of your family for a month or so. Besides figuring out how to store water while working with limited storage space, one also needs to figure out ways to gather water when the tap runs dry and how to make that water potable. Even more, if the water crisis persists, people will have to identify water sources both inside and outside their homes that can be used when the situation becomes desperate.

Communication

Taking down the Internet or disrupting the communication infrastructure remain high-priority targets since we live in a world where access to information is key to our survival.

Communications infrastructure providers are increasingly investing in cybersecurity measures and intrusion detection

systems to protect against cyber threats. Additionally, there are ongoing efforts to improve information sharing and collaboration among industry stakeholders to better respond to cyber threats.

Even so, some attacks are successful, and they show how vulnerable these infrastructures are. In 2013, a cyberattack on a large telecommunications company disrupted the phone and internet service for millions of customers in several states. The attack, which was carried out by hackers based in Asia, targeted the company's Domain Name System (DNS), which translates domain names into I.P. addresses. The attack caused widespread service disruptions and highlighted the importance of securing critical infrastructure.

In 2017, a ransomware attack on a county government in Ohio disrupted emergency communication services, including the 911 system. The attack affected the computer-aided dispatch system used by emergency responders, making it difficult for them to coordinate and respond to emergencies. The attack was eventually resolved, but it raised concerns about the impact of cyberattacks on emergency services.

In 2020, a cyberattack on a major US telecommunications company resulted in the theft of sensitive customer data, including phone numbers, addresses, and Social Security numbers. The attack, which was reportedly carried out by hackers based in China, targeted a third-party vendor that provided services to the telecommunications company.

General impact

Hacking a communication infrastructure can have significant and wide-ranging impacts. Depending on the scale and scope of the attack, it can lead to disruptions in communication networks, loss of data and sensitive information, financial losses, and even physical damage. For example, a successful attack on a telecommunications provider could lead to

disruption in phone coverage, internet access, and GPS capability for millions of people.

A cyberattack on communication infrastructure can result in not only immediate effects but also long-term consequences, such as loss of public trust and confidence in the affected companies or organizations and heightened regulatory oversight. Hence, it is imperative to implement sufficient measures to safeguard communication infrastructure and thwart hacking attempts.

What can you do?

We heavily rely on telecommunications and the Internet, and I honestly believe this will lead to our downfall since people are so imprisoned by this technology that they have forgotten how to do even simple tasks like basic math or boiling an egg. Perhaps we should teach the new generation not to rely on the Internet for everything and let them figure out things for themselves.

It’s important to have countermeasures in case of internet or communication failures, and the radio is a great alternative for news, weather, and emergency information. Local NOAA frequencies on a shortwave receiver can provide storm warnings, weather reports, and forecasts. Shortwave listening can also offer local, national, and world news. Ham radio handhelds and satellite phones are also options for communication during an emergency.

The supply chain

The scope of the global supply chain is extensive, encompassing manufacturing, the service industry, and logistics involved in the delivery of goods and services. And while there are unforeseen events, such as the 2021 Suez Canal blockage, that lead to the physical disruptions of international shipping routes, causing significant delays in

the supply chain, there are some digital threats that can have a greater impact on the distribution of goods.

A supply chain hack or attack targets the software, hardware, or third-party vendors that organizations rely on to conduct their business. These attacks can be local or global, affecting multiple organizations at the same time. In the United States, there have been quite a few cyberattacks which affected the activity of various organizations.

For example, in 2017, a supply chain attack targeted a popular accounting software used by many businesses. The attack, which was carried out by Russian hackers, enabled the attackers to steal sensitive financial information from the affected companies. The attack affected more than 100 organizations and underscored the risks of supply chain attacks.

In 2020, the Russians carried out another successful attack that targeted a widely used software development tool. The attack enabled the hackers to insert malicious code into the software, which was then distributed to many organizations. The attack affected numerous businesses and government agencies and delayed the delivery of various goods, including food.

General impact

Industrial control systems, logistics networks, and software applications, among others, are all innately susceptible to cyberattacks. The end result? Well, in a best-case scenario, there will be a shortage of your favorite snacks at your local supermarket. However, if things get really bad, you will have to wait in line with other disgruntled shoppers, even for basic foods, and figure out ways to deal with price gouging practices.

What can you do?

Preppers aim to become self-sufficient and cut their reliance on the supply chain, but this can be difficult to achieve even by the most stubborn of us. For the general public, it will be even more difficult to deal with prolonged shortages since they don’t know where their food comes from and what they should do in the absence of it.

While having a supply of essential items such as water, canned goods, medicine, and hygiene products is wise, it only scratches the surface of emergency preparedness self-sufficiency. There will be items that will be hard to find, such as spare parts for your vehicle or the machinery you frequently use. Things will break down, and you need the knowledge but also the necessary equipment and spare parts to keep them functioning.

Think about what you will do if big-box stores and online retailers will suddenly stop operating. Perhaps you have everything you need stored somewhere safe, or maybe you will discover that you need to stockpile some batteries and lightbulbs since there aren’t any to spare in your house.

Concluding

The disruption of critical infrastructures can have far-reaching effects on businesses, economies, and society as a whole. There are many attacks being orchestrated against the U.S. infrastructure, and while it may seem that everything is working as intended, we rarely find out the truth about what’s going on behind the scene and the efforts to keep the wheels spinning.

The best thing you can do for your loved ones is figure out ways to be as independent as possible and make do with the items you’ve stored or work with the preparations you’ve made. You don’t need to cut yourself completely from the public

infrastructure since going off the grid is not always possible, but you can make a plan to keep things working and provide for your family while the world around you comes to a stop.