Protect all entry points

There's a wide range of vulnerabilities and systems that need to be found.
Assessing those weaknesses is a time-consuming process.
To position themselves ahead of threats and make the most of their limited resources, companies start by understanding the environment surrounding their operations.
An important part of this is getting a sense of their attack surface.
An attack surface is all the potential vulnerabilities that a threat actor could exploit.
Analyzing the attack surface is usually the first thing security teams do.
For example, imagine being part of a security team of an old castle.
Your team would need to decide how to allocate resources to defenses.
Giant walls, stone towers, and wooden gates are a few common security controls of these structures.
While these are all designed to protect the assets inside from attacks, they don't exactly account for all the possibilities.
What if the castle were near the ocean?
If it were, these defenses would be vulnerable to long range attacks by ship.
A proper understanding of the attack surface would mean your security team equipped the castle with catapults that could deal with these kinds of threats.
Modern organizations need to concern themselves with both a physical and digital attack surface.
The physical attack surface is made up of people and their devices.
This surface can be attacked from both inside and outside the organization, which makes it unique.
For example, let's consider an unattended laptop in a public space, like a coffee shop.
The person responsible for it walked away while sensitive company information was visible on the screen.
This information is vulnerable to external threats, like a business competitor, who can easily record the information and exploit it.
An internal threat of this attack surface, on the other hand, is often angry employees.
These employees might share an organization's private information on purpose.
In general, the physical attack surface should be filled with obstacles that deter attacks from happening.
We call this process security hardening.
Security hardening is the process of strengthening a system to reduce its vulnerabilities and attack surface.
In other words, hardening is the act of
minimizing the attack surface by limiting its points of entry.
We do this a lot in security because the smaller the attack surface, the easier it is to protect.
In fact, some security controls that we've explored previously, like organization policies and access controls, are common ways that organizations harden their physical attack surface.
The digital attack surface is a bit tougher to harden.
The digital attack surface includes everything that's beyond our organization's firewall.
In other words, it includes anything that connects to an organization online.
In the past, organizations stored their data in a single location.

This mainly consisted of servers that were managed on-site.
Accessing the information stored on those servers required connecting to the network the workplace managed.
These days, information is accessed outside of an organization's network because it's stored in the cloud.
Information can be accessed from anywhere in the world.
A person can be in one part of the world, fly to another place, and continue working. All while outside of their organization's network.
Cloud computing has essentially expanded the digital attack surface.
Quicker access to information is something we all benefit from, but it comes with a cost.
Organizations of all sizes are under more pressure to defend against threats coming from different entry points.
When we get together next time, we'll explore why this is such a challenge.

Revision #1
Created 2023-08-21 09:03:20 UTC by naruzkurai
Updated 2023-08-21 09:04:34 UTC by naruzkurai