Defense in depth strategy

A layered defense is difficult to penetrate.
When one barrier fails, another takes its place to stop an attack.
Defense in depth is a security model that makes use of this concept.
It's a layered approach to vulnerability management that reduces risk.
Defense in depth is commonly referred to as the castle approach because it resembles the layered defenses of a castle.

In the Middle Ages, these structures were very difficult to penetrate.
They featured different defenses, each unique in its design, that
posed different challenges for attackers.
For example, a water-filled barrier called a moat usually formed a circle around the castle,
preventing threats like large groups of attackers from reaching the castle walls.
The few soldiers that made it past the first layer of defense were then faced with
a new challenge, giant stone walls.
A vulnerability of these structures were that they could be climbed.
If attackers tried exploiting that weakness, guess what?
They were met with another layer of defense, watch towers, filled with defenders ready to shoot arrows and keep them from climbing!
Each level of defense of these medieval structures minimized the risk of attacks by identifying vulnerabilities and implementing a security control should one system fail.

Defense in depth works in a similar way.
The defense in depth concept can be used to protect any asset.
It's mainly used in cybersecurity to protect information using a five layer design.
Each layer features a number of security controls that protect information as it
travels in and out of the model.

The first layer of defense in depth is the perimeter layer.
This layer includes some technologies that we've already explored,
like usernames and passwords.
Mainly, this is a user authentication layer that filters external access.
Its function is to only allow access to trusted partners to reach the next layer of defense.

Second, the network layer is more closely aligned with authorization.
The network layer is made up of other technologies like network firewalls and others.

Next, is the endpoint layer.
Endpoints refer to the devices that have access on a network.
They could be devices like a laptop, desktop, or a server.
Some examples of technologies that protect these devices are anti-virus software.

After that, we get to the application layer.

This includes all the interfaces that are used to interact with technology.
At this layer, security measures are programmed as part of an application.
One common example is multi-factor authentication.
You may be familiar with having to enter both your password and a code sent by SMS.
This is part of the application layer of defense.

And finally, the fifth layer of defense is the data layer.
At this layer, we've arrived at the critical data that must be protected, like personally identifiable information.
One security control that is important here in this final layer of defense is asset classification.

Like I mentioned earlier, information passes in and out of each of these five layers whenever it's exchanged over a network.
There are many more security controls aside from the few that I mentioned that are part of the defense in depth model.
A lot of businesses design their security systems using the defense in-depth model.
Understanding this framework hopefully gives you a better sense of how an organization's security controls work together to protect important

---

Revision #2
Created 2023-08-08 05:35:18 UTC by naruzkurai
Updated 2023-08-15 18:44:13 UTC by naruzkurai