Jason Palmeri

WEB 201

Professor Kumar

8/23/2021

Intranet Security

In a time when many company employees are working from home, having access to work materials is crucial in this ever-growing technological age. As employees move from the office to their own homes being able to communicate with co-workers and managers is extremely important, to keep everyone updated and on task. The Intranet is a private network used primarily by organizations to distribute communications exclusively to their employees. Throughout the years, as technology evolved we’ve come to see Intranets go from private internal organization tools, to now cloud based tools that allow the employees of their company to access their work from anywhere around the world, from any device. As the Intranet evolves to this more cloud-based system there comes many risks to the security and safety of the people using the Intranet, as well as the files and tools that are stored on the Intranet. A common problem among organizations that use the Intranet, is that they treat it as if it was something that is internal, and hidden from the public, which is far from the truth. The Intranet, like many other things is a Web application exposed to a hostile environment in the same way that a corporate website is, just because it is intended for employees and trusted parties, does not mean that is is invulnerable to hacker attacks, viruses, and spam. In today's modern world there are evil people out there who want your information, and they will try to get it in any way possible, so it is important that these Intranets have a dedicated security policy associated with them. One of the first lines of defense to, basically everything we do online, are passwords, having a strong password is a must, as hackers are able to crack passwords incredibly fast. It is always good to change your password often, and Intranets can force users to change their passwords often, to avoid and problems. A great way to keep an Intranet secure, is by deploying a layered security protocol. Jive states that “Strong intranet security should include things such as… ISO 27001 standard, regular third-party audits, and consistent updating based on industry trends” These layers of security help to ensure that the Intranet keeps up with the ever-changing security landscape. Keeping a cloud-based intranet secure can be difficult, as you won’t know who is trying to connect, which is why Identity Protocols are important. Unily says that “When you have identity protocols in place, there’s a risk of password sharing that can’t be ignored… It’s important to prioritize cryptography, data storage, legislation, and encryption”. Intranet security is top priority when deploying an Intranet in an organization, and while maintaining it can be pretty straight forward, there is always the element of human error. Employees can be a hazard to the company Intranet, and without proper knowledge and training in the subject, things can go wrong pretty quickly.

Jive. (2020, January 28). *Intranet security: Best practices for an intranet security system*. Jive Software. https://www.jivesoftware.com/blog/intranet-security-best-practices/.

Mansoor, B. (2017, May 19). *Intranet security*. Computer and Information Security Handbook (Third Edition). https://www.sciencedirect.com/science/article/pii/B9780128038437000156.

SocialChorus. (2021, August 15). *What is an intranet and is it still relevant to your organization?* SocialChorus. https://socialchorus.com/blog/what-is-an-intranet-and-is-it-still-relevant-to-your-organization/.

Unily, U. (2021, June 11). *Intranet security 101: Securing your digital workplace*. Unily. https://www.unily.com/insights/podcasts/intranet-security-101.