

The principle of least privilege: A strategy of limiting access to what is essential

The principle of least privilege is a security strategy applicable to different areas, which is based on the idea of only granting those permissions that are necessary for the performance of a certain activity

In a recent conversation with our marketing analyst at ESET Mexico, Juan Carlos Fernández, we discussed a story about a scam carried out by a bogus company during his time as a university student. The company, which allegedly recruited students, collected information included on the résumés of those who applied.

No students were actually hired, of course, but their personal information had been provided voluntarily. The incident would be quite irrelevant if it wasn't for the fact that résumés usually include personal information and data, which can compromise people's safety if it falls into the wrong hands. In the case of university students, data such as their photographs, addresses, contact information, social network accounts, and other information will no doubt be included.

And while this information may be necessary for some recruiters, it is highly likely that it is not essential when finalizing the hiring process. The idea of only providing the required information, and access to it,



discuss it in this publication.


Least privilege: A good security practice

In the area of cybersecurity, the assignment of permissions that a user may have to a system or to information is a security practice that is continuously applied. For example, operating systems are developed with different roles (and, of course, privileges), which are designed for different user profiles, based on their activities and responsibilities.

Operating under the principle of least privilege, as the name implies, is based on the premise of only granting necessary and sufficient permissions to users to carry out their activities, for a limited time, and with the minimum rights required for their tasks. This practice can be implemented with respect to technology usage, with the aim of ensuring the security of information, as well as our privacy.

Assigning permissions to users that go beyond the rights necessary to carry out a certain action may allow them to carry out actions that they are not authorized to carry out, such as accessing, obtaining, or modifying information. And privileges must also be considered for entities or services to meet their objectives without compromising privacy or security; however, for this task, an important responsibility of users is ascertaining and only granting necessary and sufficient permissions.

Can least privilege be applied to social networks?



responsibility we have as users over how our personal information is handled.


And while the paradigms of privacy change over time, we should not ignore the fact that this is a constant concern, especially in the [digital age](#), where even new legislation seeks to grant more rights to users over their information.

Based on this notion, a good practice would be to only provide the basic information necessary to use social networks and not share sensitive or confidential information with any other users, especially if we do not know those people who may be hiding behind what may be fake profiles.

So, in addition to being careful about the information we post on different social platforms, it is also a good idea to configure the privacy and security options, as well as the restrictions applicable to other users concerning the posts or data on display. We should not become so paranoid that we feel the need to stop using these new forms of communicating and interacting, especially if we advocate their conscious, responsible, and safe use, and this is where we could also apply the principle of least privilege.

The principle of least privilege on mobile devices

The applications we install on our devices must also be limited by privileges on the device. An application may be considered intrusive (or even malicious) due to the [permissions it requests when it is](#)



There are countless cases in which applications request permissions that are often not necessary for their intended function on a phone. A classic example of this is flashlight applications. These apps only turn the LED of the device on and off, so do not require access to phone information such as location, contacts, calls, or SMS messages. In this case, the principle of least privilege should also play a prominent role.

In a specific case related to this type of flashlight application, a [banking Trojan](#) was discovered that targeted Android users. Once it was installed and executed, the app requested device administrator permissions.

In addition to granting the promised flashlight function, this remotely controlled threat also sought to steal the banking credentials of its victims. No doubt, the principle of least privilege could also be applied to this scenario, by only providing the app with the minimum privileges necessary for its function.

The principle of least privilege: A security strategy applicable to different areas

Touching back on the story we initially discussed, we know that different criteria may be considered when hiring a person, but for reasons of security and also privacy, a recruiter probably should not know all of our information, especially if all that information is not handled securely.

regardless of whether it involves an operating system, a social network, an application, or, even as we proposed at the start of this publication, when submitting a résumé.



Miguel Ángel Mendoza 2 Jul 2018 - 02:25PM

Similar Articles



Facebook lays out plan to protect elections



NordVPN reveals breach at datacenter provider

Discussion

 Recommend

 Tweet

 Share

Sort by Best ▾



Start the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS 



Name

Be the first to comment.

 Subscribe

 Add Disqus to your site

 Disqus' Privacy Policy

DISQUS

welivesecurityTM BY **eset**[®]

Home

About Us

Contact Us

Sitemap

Our Experts

ESET

Research

How To

Categories

RSS Configurator

News Widget

Privacy policy

Legal Information

Copyright © ESET, All Rights Reserved

