THE UNIVERSITY OF CHICAGO

Biological Sciences
Information Security Office

July 2023

Cyber Security Awareness Newsletter

Protecting yourself and information from cyber security threats.

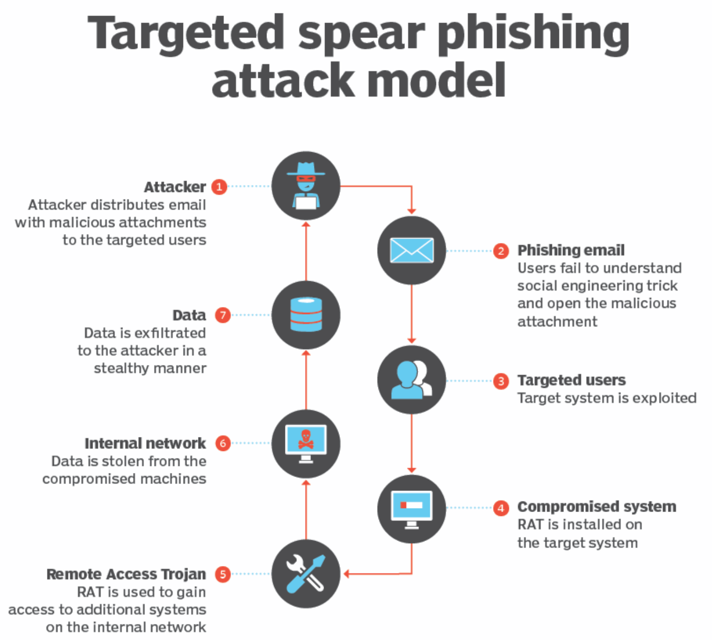
This month we want to shed light on an important topic that often gets overlooked: access rights and the implications of administrative access. Many people have their own personal computers at home where they probably use an administrator account instead of a regular user account as a primary login. Below, we'll go over some things you need to be aware of when you use an administrator account: access rights, and the dangers, responsibility, and consequences that come with having IT administrative access.

Understanding Privileged Access Management for Enhanced Security

Admin (Administrative or Administrator) rights are the highest level of privilege that can be given to a computer user. An account with administrative rights can execute almost any action on a computing system, such as installing, changing, or deleting software, services, drivers, local system accounts, and system files that are usually off-limits to a regular user. In other words, an Admin is a user with very little restriction on the whole computing system. Some people may see it as a sign of high status within a business, but in fact it is a heavy burden of responsibility to bear.

Admin Rights in Practice

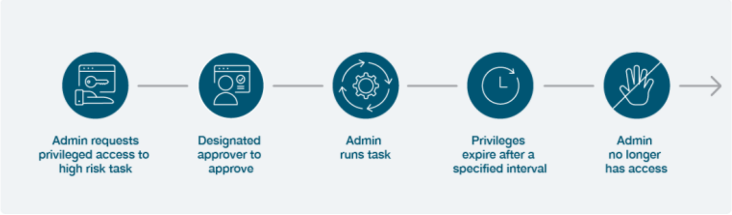
Privileged users usually have access to critical systems, databases, internal use applications, and can perform tasks, such as installing and modifying software. Having these privileges can increase productivity and efficiency as you can download an app on your device without requesting and waiting for permission from system support personnel. So why aren't privileges given out like candy on Halloween? Because a cybercriminal can compromise a device without hindrance and quickly search for sensitive information within the network. This method of information finding is the start of what a cybercriminal does for lateral movement. Example:


Targeted spear phishing attack model
Attacker 1
Attacker distributes email with malicious attachments to the targeted users
2 Phishing email
Users fail to understand social engineering trick and open the malicious attachment
3 Targeted users
Target system is exploited
4 Compromised system
RAT is installed on the target system
Remote Access Trojan 5
RAT is used to gain access to additional systems on the internal network
Internal network 6
Data is stolen from the compromised machines
Data 7
Data is exfiltrated to the attacker in a stealthy manner

Admin rights can enable a user to access information of high sensitivity, which increases the importance of the device they are using. Consequently, a user with privileged access has an increased obligation to safeguard their device, such as by monitoring for the latest security trends or engaging in training sessions on the proper use of admin rights.

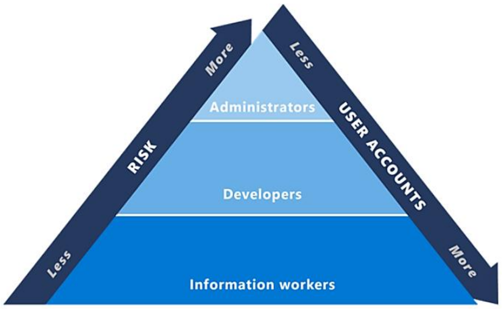
To maintain security, there are principles and policies in place to specify how privileged access can be granted and monitored.

- Least privilege - only giving as much access as needed to complete the job.
- Separation of duties - access is limited so that no single person has all administrative control. Therefore, if a device is compromised, then that one security breach is less likely to compromise the entire organization.


Admin requests privileged access to high risk task
Designated approver to approve
Admin runs task
Privileges expire after a specified interval
Admin no longer has access

- Just-in-time - you are granted privileged access, but just for a set period. (We are currently evaluating a solution for this. More to come in a future newsletter.)
- Just-enough access - the principle of least privilege. (we'll discuss his later)

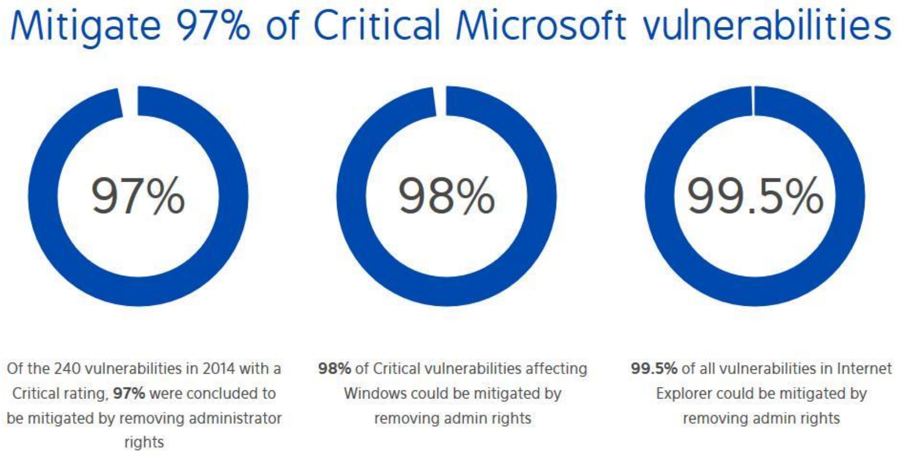
Responsibility, a Best Practice and Risks Involved



The risk-role pyramid.

We have heard this quote in movies from thinkers and leaders: "*With great power comes great responsibility.*" This quote originates from a collection of decrees made during the French National Convention in 1793, which mention that leaders "*must consider that great responsibility follows inseparably from great power."* This holds true in every aspect of computing: Giving administrative rights to more folks than necessary increases the risk of potential compromise to an organization.

As mentioned earlier, a cybercriminal can take over a device in a very short time when admin rights are found. Besides admin rights however, one of the arsenals that a cybercriminal looks for are zero-day vulnerabilities. A zero-day vulnerability is a security flaw that is unknown to vendors or software developers and as a result there is no patch to mitigate it. Zero-day vulnerabilities coupled with admin rights are very often main objectives that are actively exploited by cyber criminals. Suffice it to say, the fewer individuals who have administrative rights, the better off an organization is. In 2014 Microsoft noted in an article regarding Microsoft critical vulnerabilities:



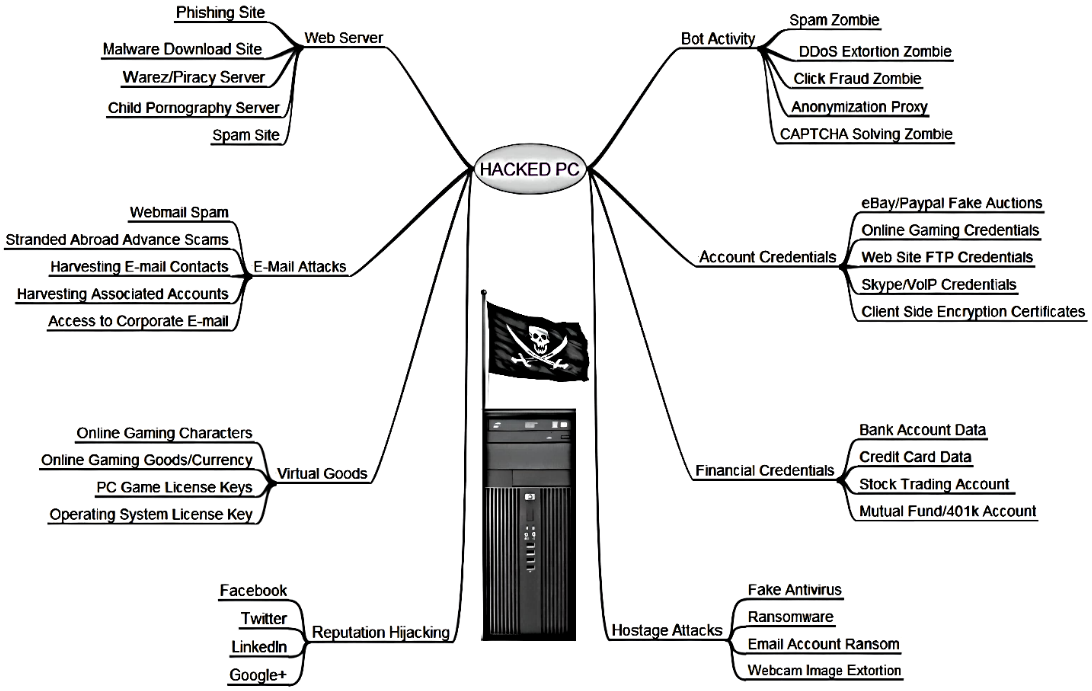
Mitigate 97% of Critical Microsoft vulnerabilities

Of the 240 vulnerabilities in 2014 with a Critical rating, **97%** were concluded to be mitigated by removing administrator rights

98% of Critical vulnerabilities affecting Windows could be mitigated by removing admin rights

99.5% of all vulnerabilities in Internet Explorer could be mitigated by removing admin rights

The principle of least privileged is an information security best practice that gives users, typically employees, the minimum level of access needed to complete their job responsibilities. This concept is practiced in the NIST Cyber Security Framework, HIPAA, ISO/EC 27001, Sarbanes Oxley, PCI DSS, GDPR and other regulations which can be included in data usage agreements especially where sensitive information is being used. Not fulfilling this principle as a responsibility can be a “red flag” to many organizations and can be cause for fines, reputational damage, legal actions and more. The black flag shown below depicts the dangers of what can happen with a compromised account that has elevated privilege.



For more information about BSD security policy regarding administrative rights please see the following web page: Access Control Policy

As always, we welcome your feedback. If you have any suggestions for topics that you would like us to cover in the next newsletter, please send us an e-mail at security@bsd.uchicago.edu.