thycotic

BLACK HAT 2017

HACKER SURVEY REPORT

Based on a survey of attendees at the Black Hat Conference – July 25-27, 2017 in Las Vegas, Nevada

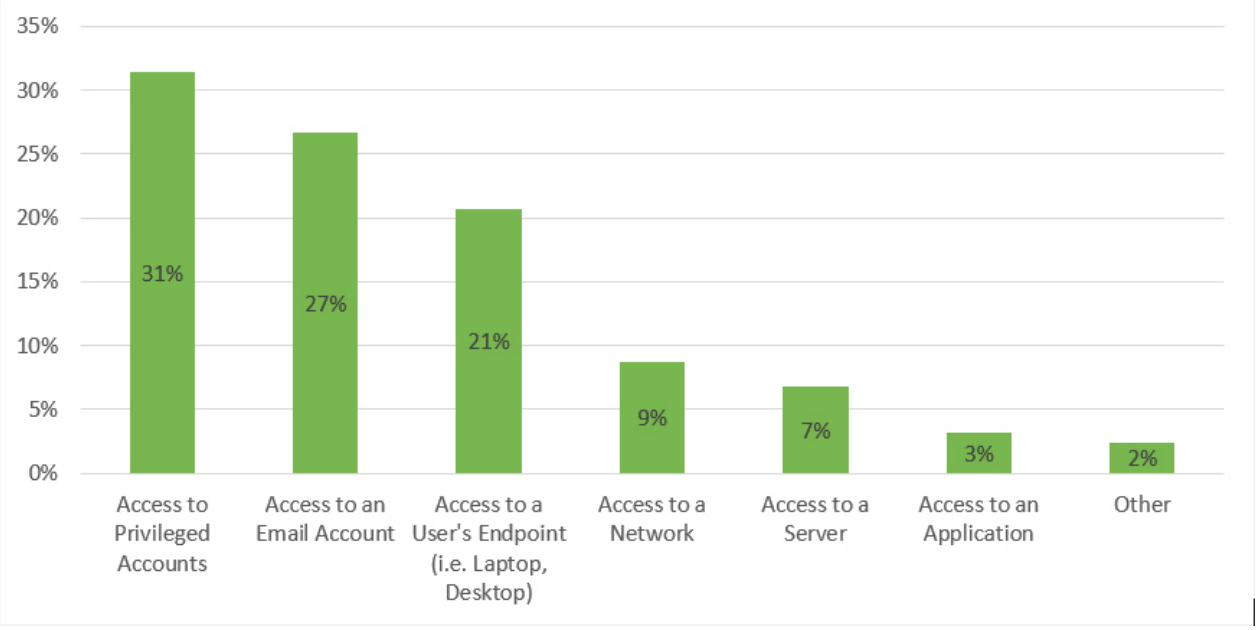
ONE-THIRD OF HACKERS SAY ACCESSING YOUR PRIVILEGED ACCOUNTS IS THE EASIEST PATH TO CRITICAL DATA

With traditional anti-virus and firewalls considered obsolete, hackers are targeting privileged accounts and email users.

At the largest cyber security event of the year, Black Hat 2017 in Las Vegas, Thycotic surveyed more than 250 hackers to get their take on what works and doesn't work when it comes to protecting critical data.

? Which entry point gives you the easiest / fastest access to sensitive data?

Nearly one third (32%) of survey respondents said accessing privileged accounts was the number one choice for the easiest and fastest way to get at sensitive data, followed closely by 27% indicating access to user email accounts was the easiest path to capturing critical data.



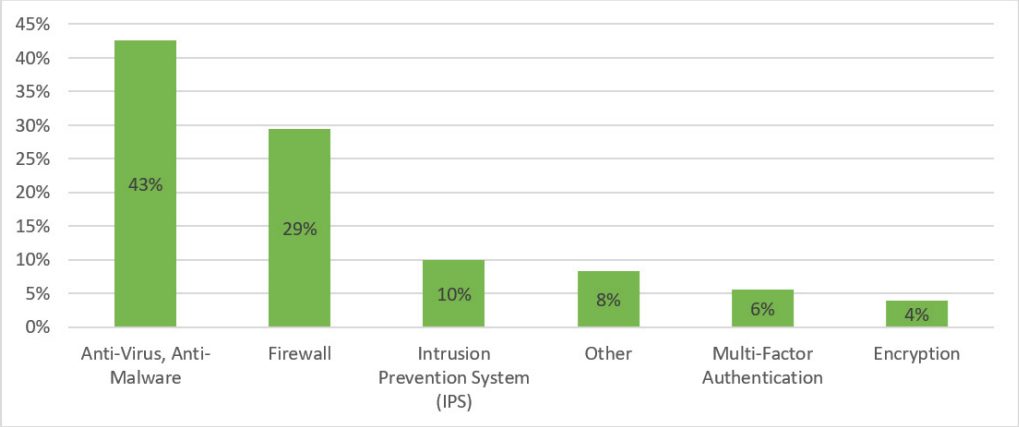
QUESTION

Which entry point gives you the easiest / fastest access to sensitive data?

73% say traditional perimeter security firewalls and antivirus are irrelevant or obsolete

The focus on hacking privileged and email accounts reflects a recognition on the part of hackers that traditional perimeter security is no longer a barrier to getting inside networks and gaining access to critical data.

Anti-virus and anti-malware are considered the "least effective and easiest to get past" security technologies by 43% of the Black Hat survey respondents, followed by 30% of Black Hat respondents naming firewalls the easiest security technology to get past.

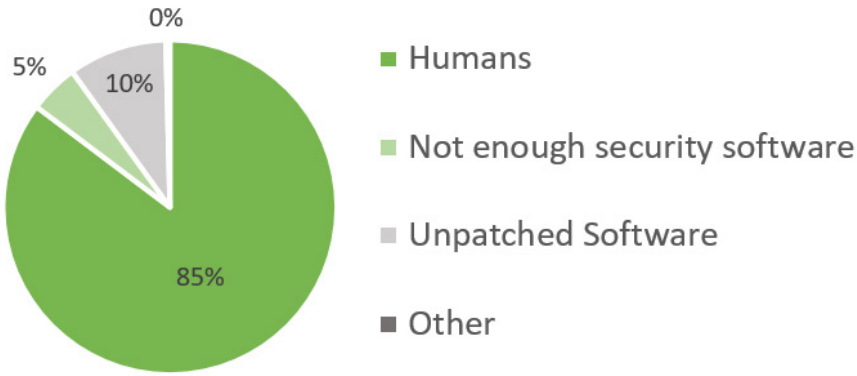


QUESTION

Which of the following is most responsible for security breaches?

More than four out of five blame humans for security breaches

With perimeter security technologies considered largely irrelevant, hackers are focusing more on gaining access to privileged accounts and email passwords by exploiting human vulnerabilities. Indeed, more than 85% of Black Hat survey participants named humans as most responsible for security breaches. Unpatched software (10%) and insufficient security technology (5%) were far behind.

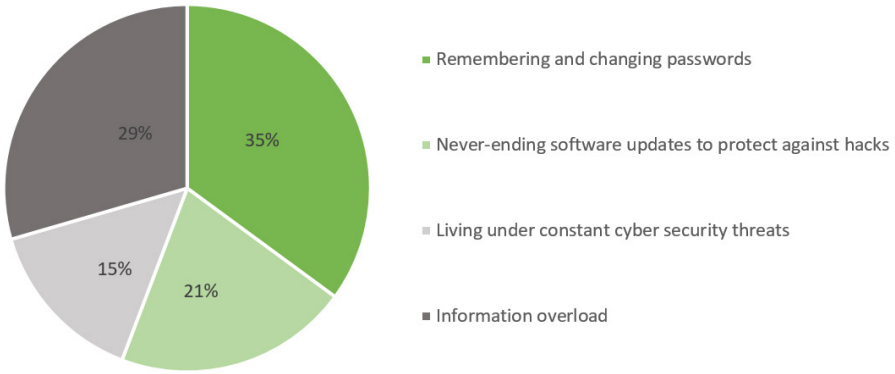


QUESTION

What is the biggest source of cyber fatigue?

Hackers cite "remembering and changing passwords" as top source of cyber fatigue

One reason humans readily get the blame for security breaches is the constant pressure on users, which frequently results in cyber fatigue–a condition where human users fail to follow proper cybersecurity hygiene when executing daily tasks. More than a third of survey respondents (35%) said that "Remembering and changing passwords" was the top source of cybersecurity fatigue, a major vulnerability that hackers are all too willing to exploit. Other contributing factors included "Information overload" (30%), "Never ending software updates" (20%) and "Living under constant cyber security threats" (15%).

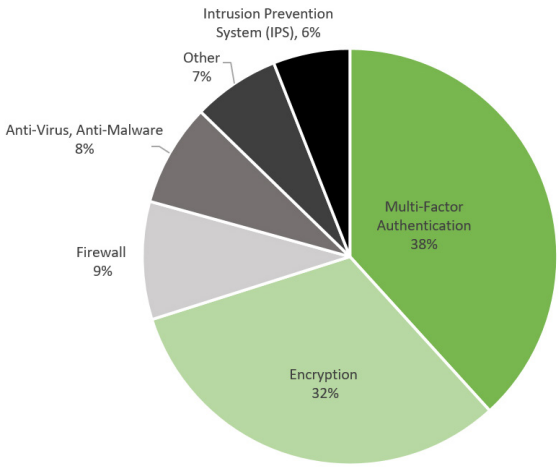


QUESTION

What type of security is the hardest to get past?

Multi-factor authentication and encryption are biggest hacker obstacles

As hackers increasingly target privileged accounts and user passwords, it's perhaps not surprising that the technologies they considered the toughest to beat include Multi-Factor Authentication (38%) and Encryption (32%), with endpoint protection and intrusion prevention far behind at 8% and 5 % respectively.

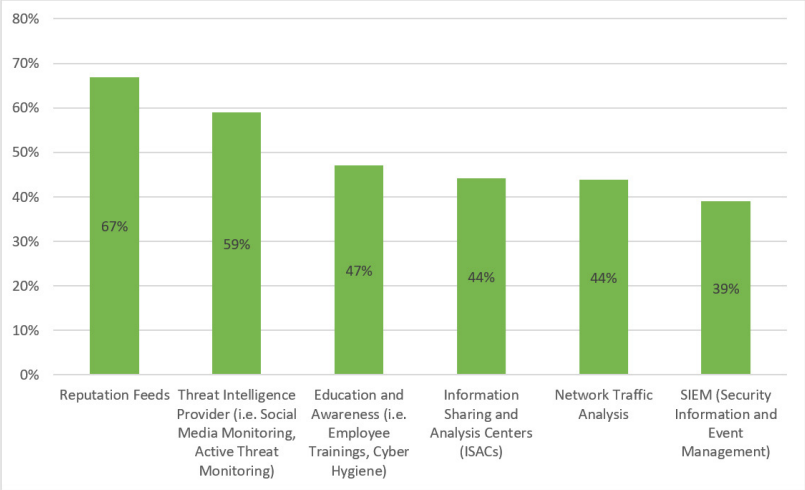


QUESTION

Which three Threat Intelligence options offer the least protection?

Threat Intelligence not so smart?

While Threat Intelligence solutions have become a major trend in proactively detecting insider as well as outside cyber threats, hackers viewed them as one of the least effective security protections, along with reputation feeds and education/ awareness. Because Threat Intelligence solutions are also accessible to hackers, they may be able to easily identify how they work and therefore avoid detection them. The reduced effectiveness of threat intelligence may also be due to the lack of a clear strategy or visibility into their cyber security metrics. See the new 2017 State of Cybersecurity Metrics report at thycotic.com/cybersecuritymetrics/ to see where companies are most struggling when it comes to cybersecurity and monitoring.

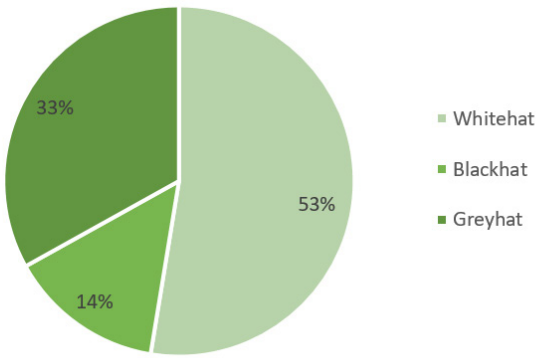


QUESTION

What type of hacker do you most identify with?

Most survey respondents identify as White Hat hackers

This years' annual Black Hat survey asked what type of hacker our respondents most identified with. Among survey participants this year, 51% consider themselves as White Hat hackers using their skills for good. Another 34% identified themselves as Grey Hat hackers applying their skills for both good and bad causes, and 15% self-identified as Black Hat–hackers who break into computer systems and network with malicious intent.



SURVEY RESULTS SUGGEST PRIORITIZING IDENTITY AND ACCESS MANAGEMENT SECURITY

In today's connected, always on world, organizations can no longer rely on traditional perimeter cyber security measures. The new cyber security "perimeter" incorporates a human firewall built around employee and third-party Identity and Access Management education and technology controls. This new cyber security defense emphasizes the protection of privileged account credentials and user passwords across the enterprise with automated solutions that reduce complexity and user fatigue while enhancing ease of use and user productivity.

The Black Hat survey results are a wakeup call for organizations to bolster their cyber security efforts by:

- Educating all key stakeholders on the fundamentals of cyber security.
- Taking a people-centric approach to cyber security that prioritizes ease of use and less complexity.
- Implementing Multi-Factor Authentication for emails and all sensitive privileged accounts.
- Enabling encryption to protect user credentials and privacy.
- Automating the management and security of privileged accounts.

NEXT STEPS

Given that privileged accounts are prime targets for hackers, IT professionals should consider the opinions of the hackers themselves when it comes to protecting privileged account access. Thycotic provides innovative free tools and automated PAM security products that deliver simple, easy to use and affordable solutions to protect your privileged accounts and user passwords while improving the security of your IT infrastructure. You can learn more by visiting thycotic.com/free-tools/ . Based on this year's results, we recommend our Browser Stored Password Discovery Tool and Windows Privileged Account Discovery Tool to measure your risk, and our Password Policy Template to help you standardize the human processes.

SURVEY METHODOLOGY

In July 2017, Thycotic surveyed 250+ attendees including self-identified hackers live at the Black Hat 2017 conference in Las Vegas. "Hackers" were defined as official attendees of the Black Hat conference who personally identified themselves as a hacker at the time of the poll. Respondents remained anonymous to protect their personal identity. For more information, please email sales@thycotic.com.

ABOUT THYCOTIC

Thycotic, a global leader in IT security, is the fastest growing provider of Privilege Management solutions that protect an organization's most valuable assets from cyber-attacks and insider threats. Thycotic secures privileged account access for more than 7,500 organizations worldwide, including Fortune 500 enterprises. Thycotic's award winning Privilege Management Security solutions minimize privileged credential risk, limits user privileges and controls applications on endpoints and servers. Thycotic was founded in 1996 with corporate headquarters in Washington, D.C.and global offices in the U.K. and Australia. For more information, please visit thycotic.com .