SecureAuth have found that 39% of UK IT decision makers only use passwords as an IT security measure

Contributed by SecureAuth
Wednesday, 18 March 2015

- A third (33%) of companies with more than 1,000 employees are still using password only access
- 45% of public sector organisations use password only based security
- Half (54%) are concerned that employees could compromise access to their corporate network
- A third (33%) of employee's time is spent accessing the organisation's IT network remotely
- A third (28%) of IT decision makers believe businesses will use biometrics as an IT security access measure in 5 years' time

New research from access control innovator, SecureAuth, shows that despite much debate, the password isn't dead yet as two in five IT decision makers (ITDMs) admit that passwords are their only IT security measure. It is a worrying revelation, considering the prevalence of security breaches due to compromised credentials.Â Furthermore, a third (33%) of companies with more than 1,000 employees are still using password only access.Â Even more concerning, one in five (20%) respondents said they â€˜don't know' how many IT security policies their company currently has.

The entertainment, hospitality and leisure industry is taking the most risks with its data as two thirds (65%) of respondents from this sector admit their organisations only use passwords as a security method.Â Additionally, almost half (45%) of ITDMs from public sector organisations revealed they also only use passwords - a concern considering organisations in this sector are responsible for protecting the public's sensitive information.

It appears that organisations in all sectors aren't always aware of the inherent risks of using password-only access, with over half of businesses (54%) requiring their staff to change passwords less frequently than every two months.Â Almost a quarter (24%) admit that passwords are changed less than two to three times a year.

Despite companies relying on passwords alone, the survey revealed that the majority of ITDMs (63%) are confident that their current authentication methods are effectively protecting valuable assets.

Those in the IT and Telecoms industry were the most clued up on methods of protecting their data with almost three quarters (74%) stating that they don't use solely password-based security.

"It's extremely concerning just how many businesses still use passwords as their only method of protection against malicious hackers and the false confidence they seem to have in their current security systems is only further cause for concern," commented Nick Mansour, Executive Vice President of Worldwide Sales at SecureAuth.

"Over the last 12 months, there have been an incredible number of data breaches occurring where lax access controls and the theft of credentials have played a key part in the loss of sensitive data.Â These organisations who are continuing to blindly use passwords alone to secure their corporate networks need to wake up to the fact that there are a number of inherent risks that come with relying on using passwords to protect valuable data.Â Organisations of all sizes, from all sectors, should be doing more to address these issues," continued Mansour.

The threat from within

Businesses are not just facing threats from outside the organisation but also from within.Â More than half (54%) of respondents said that they are most concerned that employees could compromise access to their corporate network, whether intentional or not.Â However, one in five (21%) ITDMs in the manufacturing industry believe that suppliers and partners pose the most risk to the corporate network.

The flexible working model and BYOD are becoming more commonplace, with two in five (42%) respondents claiming that employees are now accessing corporate systems through three or more devices and a third (33%) of an employee's time is spent accessing the organisation's IT network remotely - the equivalent of at least 612.3 hours a year* per business worker.Â However, despite the popularity of remote working, almost one in five (17%) organisations don't see the need for additional access control and have just one method in place and 44% of respondents stating that their organisation has two or fewer methods in place to deal with remote access.

The survey also revealed an almost even split in which resources ITDMs are the most concerned about protecting.Â Almost a third (28%) stated that protecting on premise applications is a top priority, closely followed by 29% citing that they are most concerned about safeguarding the company's Virtual Private Network (VPN).Â One in five (20%) stated Cloud and SaaS is the most important company resource to protect and 18% said mobile takes precedence.

However, the research indicated that different sectors have different priorities - ITDMs in the manufacturing industry are the most concerned about mobile access (24%) but those in the public sector are far more concerned with VPN access (29%) and one in five ITDMs (22%) in the professional and financial services sector claim they are most concerned about cloud and SaaS access.

Access controls and the future

Less than half (44%) of respondents have plans to change or enhance their security model in the next two years with just over one in ten (12%) stating they don't know if they're planning to change their current access methods - suggesting that IT access security is not keeping pace with the increasingly sophisticated ways in which criminals are targeting enterprises. Â

As biometrics become more commonplace on our smartphones and tablets, nearly a third (28%) of IT decision makers believe that businesses will use this as a security measure in 5 years' time.Â The survey indicated that it will take 5 years before we see a significant shift in organisations' reliance on passwords alone and passwords and tokens.Â Respondents expected to see a 62% drop in the use of passwords alone and a 58% drop in passwords and tokens.Â However, a quarter (24%) said that they â€˜don't know' what the future will hold for authentication.

Mansour continues, "We've seen many instances of companies not being stringent enough with their security access control and what's becoming clear is that organisations are slow to adapt to the demands of the ever changing IT landscape.Â As the skills of hackers continue to evolve, organisations are going to have to wise up to new methods of information access security, such as adaptive authentication which can leverage real time threat intelligence, biometrics and even behavioural analysis.Â The findings of this survey confirm there is a huge need for businesses to adopt more modern access control strategies if they want to ensure their sensitive data remains safe, both now and in the future."

The research

The research, conducted by Opinium for SecureAuth, studied the approach businesses have to their IT security and access control and all figures, unless otherwise stated, are from Opinium.Â Total sample size was 500 IT decision makers in organisations in the UK with 50 or more employees.Â Fieldwork was undertaken between 20th February and 4th March 2015.Â The survey was carried out online.

*Based on an average 8 hour working day and 233 working days a year excluding bank holidays and 20 days annual leave