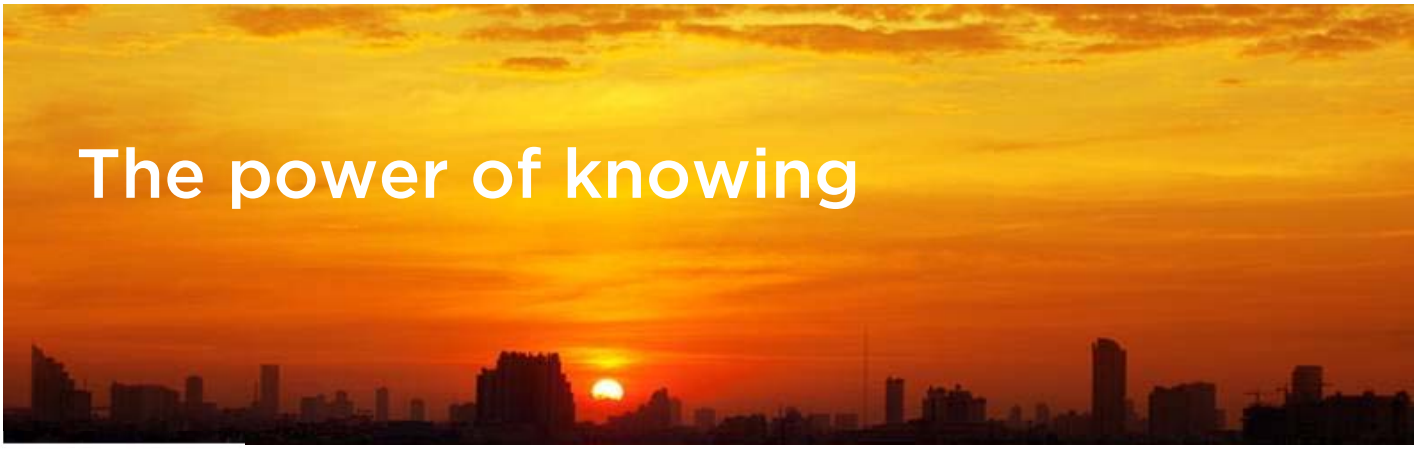

The power of knowing

This Danish based multi-national business is one of the largest companies in the world; operating in 125 countries and employing over 100,000 people they play a critical role in the global economy that can have an impact on the day to day lives of virtually every person on the planet.

The Challenge

Managing such a large and complex operation is a mammoth logistical and administrative task that depends heavily on a sophisticated global IT infrastructure linking its 325 worldwide offices to its European data centre. In addition the company employs a large mobile workforce which also needs regular access to the network to ensure the smooth running of the operation, from a variety of different and constantly changing locations.

As a critical requirement of their business, the company has invested heavily in the latest network technology that needs to deliver maximum performance and round the clock availability to ensure access to mission critical applications and sensitive data, whenever it is required.

With such a large and widespread network of remote users, the company naturally takes the issue of security extremely seriously. As well as incorporating the latest endpoint security technology to protect the network perimeter and corporate applications from malware or attack, the company also recognises that a strong user authentication system is essential to ensure that only authorised personnel are allowed access to the specialist applications and commercially sensitive data needed for the smooth operation of a worldwide business operation.

Having initially designed and operated the network based on using a key-fob based token technology to secure the user log-in process, the company's IT team were finding the system increasingly difficult to administer; restricting the wider development of the network and generating significant support issues. In particular, provisioning the system to a worldwide user base created a major administrative task both to add and delete new users as well as managing the 3 year replacement life-cycle of the tokens.

Following a major Group acquisition, which meant the addition of several thousand new network users, the company decided that there was an urgent requirement for a more flexible alternative authentication technology that could better scale to the company's future and growing needs, without compromising security. With guidance from the Information Security Forum (ISF), the global, independent advisory organisation, and the Danish systems integrator, Betech Data, the company selected the Swivel multi-factor authentication technology as its preferred solution.

T: +44 (0) 1937 582020 E: hq@swivelsecure.com
Swivel Secure Ltd, Equinox 1, Audby Lane, Wetherby LS22 7RD
swivelsecure.com

Solution

The Swivel Authentication Platform is a flexible alternative to token based authentication systems and includes a range of options leveraging existing Internet connections or mobile networks to enable users to generate a one-time access code each time they need to login to the secure network.

As with the company's old system, Swivel includes the need for each user to have a unique, four-digit PIN number, which they must keep secret. However instead of using a special hardware token the PIN number is combined with a randomly generated 10 digit alpha-numeric security string, sent to the user via a Web browser or an out-of-band SMS message to a standard mobile phone. The string and the PIN are combined to generate a new access code, which is unique to that session and cannot be re-used.

For practical and logistical reasons the company has chosen to phase in Swivel initially starting with 25,000 of its users replacing their tokens once their current licence has expired. The rest of the 100,000+ work force will be gradually moved to the technology over the next 2 to 3 years to create a standardised system across the whole Group infrastructure.

Swivel provides a second layer of user authentication in addition to the normal username and password logon procedure. The company has chosen to deploy Swivel with the option to use either the browser interface or the SMS function for maximum flexibility and to ensure that personnel can log on regardless of where they happen to be.

Due to the nature of the company's core business, users can find themselves in isolated, remote locations with limited access to a cellular mobile network for extended periods. Having both options ensures that they have a backup system when needed.

When using the browser, the security string is sent on-demand direct to user's desktop, in the form of an obfuscated GIF, once the authentication process has been initiated. The SMS version delivers the string as a standard text message onto the mobile device after authentication has been completed, ready for the next session. The latest release of the system includes the option to have multiple strings sent in one message to further extend this functionality.

Delivery

The implementation of the new remote access system is being managed by Betech Data together with the company's extensive in-house IT team and support from Swivel's technical consultants; minimising any potential disruption to the company's core operations and ensuring a smooth transition from the old system.

Return on Investment

Since the completion of the first phase of the technology upgrade the IT team has seen marked improvements in the administration and support of the remote access infrastructure:

User Provisioning

One of the major benefits Swivel has brought to the company is the ability to add and delete users centrally via a simple management dashboard, which for such a large organisation can be a significant daily task.

Previously under the old system there was the added complication of managing the distribution of tokens across the worldwide organisation, which had become a logistical nightmare for the IT staff. This was in addition to the frequent requests for the replacement of lost, stolen or faulty tokens, which as well as being time consuming was also an expensive drain on the IT budget.

Transition to the new system for the first batch of users has been a relatively smooth and trouble free operation. From the user perspective the process of extracting their OTC from the security string has proved to be easy to adapt to and without the need to worry about where their token is the users no longer need to worry that they will be locked out of the network at a crucial operational moment.

T: +44 (0) 1937 582020 E: hq@swivelsecure.com
Swivel Secure Ltd, Equinox 1, Audby Lane, Wetherby LS22 7RD
swivelsecure.com