ComputerWeekly.com TechTarget E-guide

CW+ Content

CIO Trends #11: Benelux

In this e-guide

In this e-guide:

The Netherlands is a nation leading the world in terms of digital, so it is to be expected that bit also leads the works in securing digital assets.

The country rubs shoulders with the biggest economies in the world in terms of research when it comes to cyber-security, but it appears its main airport Schiphol is not only making the country open to business, but might be opening it up to cyber-attack. In this e-guide read about a report that has damning conclusions on the IT security of some of the airport's core systems.

Report reveals inadequate cyber security at Schiphol Airport

Kim Loohuis

The cyber security of border controls carried out by the Dutch Royal Military Police at Schiphol is inadequate and not future-proof, according to a report.

Research carried out by the Dutch Court of Audit (Algemene Rekenkamer), found that security tests on the IT systems hardly ever take place, if at all. It also said the software of two IT systems is operational without the required approval, and that IT systems are not connected to the detection capacity of the Ministry of Defence and Schiphol itself.

With almost 80 million passengers a year, Schiphol is not only the most important airport in the Netherlands, but also an important gateway to Europe. The Royal Military Police check passengers entering or leaving the Schengen zone at the airport. In doing so, systems process the personal data of passengers from across the world. This includes information about nationality, travel itinerary, travel company and, in some cases, criminal data.

Passengers are checked at the passport desk and via electronic self-service gates. Travellers from outside the Schengen area are also screened with pre-assessment before arrival.

With border control, the Royal Military Police contributes to the security and control of immigration into the Netherlands. The importance of IT in border control is huge, and growing and digitisation makes it faster and more thorough – but at the same time, it creates dependence and new risks.

The passport counter, electronic self-service gates and the pre-assessment stage each have their own IT systems. The Minister of Defence is responsible for the cyber security of the systems that carry out checks on arriving passengers during their flight, and at the counters of the Royal Military Police at Schiphol. Meanwhile, the Minister of Justice and Security is responsible for the IT system of the self-service passport control at the airport.

The cyber security of these three systems is crucial to combat digital sabotage, espionage and crime. If border control IT becomes unusable due to a digital attack, the Royal Military Police can barely carry out border control, if at all. This can result in long queues, delays or flight cancellations. In addition, foreign security services can use cyber espionage to access the data of specific travellers. cyber attacks can also be used to manipulate information for wanted persons can cross the border more easily.

Not approved

The Court of Audit’s examination shows that the operation of cyber security measures is not functioning as it should. For example, the defence security policy describes the security measures that all border control IT systems must comply with and that IT systems should only be used once these measures have been taken.

However, two of the three border control IT systems have not been found to be adequately protected against cyber attacks. The passport counter system and the self-service system did not go through the Ministry of Defence’s approval procedure to establish this.

Specialists can quickly detect cyber attack by continuously monitoring IT systems. The Ministry of Defence and the Schiphol company both have such detection capabilities in the form of a Security Operations Centre (SOC).

The IT systems that support border control are not themselves connected to the detection capacity of these SOCs. As a result, there is a risk that cyber attacks on these IT systems will not be detected or will be detected too late, according to the Court of Audit report.

Insufficient testing

Defence policy also prescribes annual security tests, but in practice little or no security tests have been carried out on the three IT systems of border control.

They have never even been carried out on the pre-assessment and passport desk systems.

Several public and private parties are involved in the self-service control IT system, which is owned by the Ministry of Justice and Security. As a result, a joint security test was laborious and resulted in a smaller number of tests than the parties intended.

The various parties involved are also dependent on each other when it comes to approving the security of the system, therefore unknown vulnerabilities can remain in the system and be abused for cyber attacks.

As the Ministry of Defence had never done this before, the Netherlands Court of Audit performed a security test on the pre-assessment systems for the submarine.

The starting point for this test was the insider threat, in which the attack is carried out via a defence employee who has access to the Ministry's network but is not authorised for the pre-assessment system. This is a real risk, with 60,000 defence staff members given access to the network.

This security test revealed 11 vulnerabilities, including the use of weak passwords and the ability to send emails on behalf of random Ministry of Defence employees.

In addition, the test showed that different vulnerabilities could be combined in the event of a single cyber attack. With an advanced attack, it would be possible for unauthorised persons to manipulate the pre-assessment system in such a way that it would appear that a passenger is not, for example, on an investigation list, despite this being the case. The Ministry of Defence has now resolved these vulnerabilities, so that this attack is no longer impossible.

Not connected to SOC

The Ministry of Defence has extensive procedures for dealing with IT disruptions and crisis situations. These include specific procedures for disruptions caused by a cyber attack.

The organisation even carries out exercises with digital crisis situations. However, there is a lack of preparation based on concrete scenarios, such as an attack with ransomware and there has never been a cyber exercise for border control. As a result, it is uncertain whether the Ministry's response to a cyber attack in border control is effective in practice, concluded the Court of Audit.

Furthermore, the organisation is concerned that the IT system for pre-assessment is not connected to the detection capacity of the Ministry of Defence's SOC. The Ministry itself has identified this system as a critical system.

Border control will be further digitised in the coming years. The complexity and dependence on IT is growing. With this future in mind, it is now important to guarantee an adequate level of cyber security, the Netherlands Court of Audit stated in its report.

The Ministry of Defence already has the necessary knowledge and expertise for this. The recommendations made by the investigators in the report therefore mainly boil down to actually doing what is already possible. According to the Court of Audit, it is incomprehensible that this has not yet happened.

Already taking steps

In response to the report of the Court of Audit, Ministers Ank Bijleveld (Defence) and Ferd Grapperhaus (Justice and Security) said, in view of the increasing use of IT systems in border control at Amsterdam Airport Schiphol, further improvements are desirable.

They endorse the recommendations made by the Court of Audit in the report. “At the same time, the task in the area of cyber security is major and the IT landscape for border control is dynamic. We are already taking steps in response to many of the recommendations,” said the response to the report.

For example, the Court of Audit recommends that the necessary security measures be taken as soon as possible and that the approval procedure for the counter control system and the self-service system be completed.

According to the ministers, adjustments are currently being made to the system and additional security measures are being taken in order to better guarantee the availability of the systems in the future.

With regard to connecting to the detection capacity, the ministers state that not all systems can be connected to the SOC at the same time, and that a step-by-step approach has been adopted.

"Priority will be given to those IT systems that have the highest priority for defence. Currently, priority is given to other critical systems, with a higher degree of urgency. The network on which the systems at the desk and during the pre-assessment are located has been connected to the SOC. This already mitigates some of the risks," the ministers said in their response. In time, the other individual systems will be connected.

According to the ministers, the recommendation to carry out annual security tests is not feasible due to the limited staff capacity and the time required to follow up all findings. Incidentally, this does not apply to the self-service system. A new security test will be carried out as soon as possible and from 2021 onwards must be tested annually. In addition, it will be examined how the parties involved can practise with crises as a result of a cyber attack at Schiphol.

Coronavirus: Dutch Covid-19 tracking app stirs national debate

Kim Loohuos

Since its schools closed, the Netherlands has been in what is described as an intelligent lockdown and the government is looking at technology as a means to gradually get out of this situation.

Countries have entered lockdown one by one to limit the spread of Covid-19, with the Dutch being told take protection measures against the deadly virus in mid-March.

During a recent press conference on the current coronavirus situation in the Netherlands, public health minister Hugo de Jonge said technology could help to control the spread of the virus, with an app to trace Covid-19 cases by researching contacts between people being an obvious example.

Using Bluetooth, an app user’s phone could register automatically if it has been in the vicinity of a person who has tested positive for the virus. These Bluetooth connections would be stored locally under a unique number. The corona app could then load a list of unique numbers where a virus infection has been detected.

If someone is infected, they can indicate this in the app and a message will be sent to the numbers with which their phone has recently made a Bluetooth connection.

But such an app is not without controversy in the Netherlands. For example, privacy and security are important aspects in developing the app, which has proved something of a problem. The Dutch government called on developers to submit proposals, and about 750 did so, of which seven made a short list and were presented to the public and experts in an Appathon, but experts were immediately critical.

The government has formulated important requirements covering contact research, privacy and information security, but Brenno de Winter, a well-known Dutch privacy and security expert, does not think the apps will meet these requirements. “Input has been skilfully ignored,” he said, told newspaper *Algemeen Dagblad*. “There are now initiatives that we have dismissed as insufficient in the area of privacy. I wasted a whole day yesterday – this is a mess.”

Peter Boncz, researcher at the Centre for Mathematics and Computer Science and professor at the Free University of Amsterdam, is also surprised by the seven short-listed apps. He says a better alternative is already available from DP-3T. “But they haven’t selected it, which is a big mistake,” he told *Algemeen Dagblad*. “DP-3T has launched a fairly complete app and is working towards a pilot in Switzerland next week.”

Not surprisingly, none of the seven selected apps passed the selection criteria during the Appathon. According to Benjamin Broersma of the Open State Foundation, in a message on news site NOS.nl, all the apps have design flaws. KPMG researchers have also found many security problems in six of the seven apps – the developers did not program securely and took hardly any security measures, they said. This became painfully clear when one of the apps, Covid-19 Alert, had to report a data breach in which almost 200 names, email addresses and encrypted passwords of another app to which this app is linked were online.

"We made the source code public as soon as possible," said a Covid-19 Alert spokesperson. "In the process, we accidentally put this data online." This appears to illustrate that haste can lead to carelessness – which is exactly the fear of the privacy and security experts watching this development.

IT audit professional Thomas Wijsman has stated in a contribution on LinkedIn that the mix of high ambitions, a political deadline, a mindset of ICT-as-quick-fix and fragmented specifications are a proven recipe for turning an ICT project into a problem case.

Sixty Dutch scientists have written to the government ministers involved in the development of a corona app, expressing their fears. They wrote that the use of apps in the current crisis is far-reaching, so it is important to critically examine the usefulness, necessity and effectiveness of such apps, plus the social and legal impact, before the authorities decide to use them.

The scientists also stressed that technology is rarely the solution to a particular problem.

Many questions about the app have also been raised by Dutch citizens, such as will they be obliged to use it in the future, and who will be able to view the stored data? Also, how far can employers go in requiring their employees to install the app before they are allowed to return to the office?

According to Bert Hubert of IT infrastructure company PowerDNS, the big problem is the government's lack of expertise. "If this wasn't about software, but about a dike, things would have gone a lot better," he told website NOS.

False alarm fears

One of the concerns raised by privacy expert Lokke Moerel, professor at Tilburg University, in the *Volkskrant* newspaper is that a Covid-19 app can give a lot of false alarms, or even no alarm when there should be one. She agreed that technology is only one of the tools in the fight against the virus, but it is not a holy grail. "If you lift a lockdown with the idea that an app can control the infections, you create a false sense of security," Moerel told the *Volkskrant*.

But the Netherlands government will not give up on developing an app. During a press conference on 21 April about the current Covid-19 restriction measures in the Netherlands and possibly easing them, prime minister Mark Rutte said: "We don’t have to start all over again [with the app]. I see the current developments as the next step.”

Ministry of health director Ron Roozendaal, who deals with the introduction of Covid-19 apps, shared Rutte’s opinion, saying: “We don’t have to go back to square one. I see the events of the last few days as an ongoing process.”

The Dutch government expects to be able to decide in a month’s time whether, and how, an app can be used for contact research. Health minister de Jonge wrote to the Tweede Kamer (Lower House of Parliament) that he was “pleased” that the Appathon had led to a broad social debate. “I don’t take lightly the introduction of digital support for source and contact tracing,” he wrote. “I will not compromise on the preconditions. The possible introduction of apps will have to be accompanied by scientific research.”

De Jonge’s letter added that a new team is being set up to work on a new solution. “My commitment is to quickly have a team with the right builders and also with experts in the field of information security, privacy, fundamental rights, national security and inclusion,” he wrote.

Eurostar to roll out facial recognition for ‘passport-free’ travel to Europe

Laura Middag Alvarez,

Eurostar is to deploy biometric facial verification by iProov to allow Eurostar passengers to check-in and board without showing their passports.

By March 2021, travellers at London’s St Pancras International Station will be able to walk down a contactless, camera-lined “biometric corridor” without presenting any formal identification.

Passengers can opt to verify their identity in advance by uploading a selfie and a photograph of their passport, after which they receive a message to confirm their identity document has been secured.

The government-backed system is intended to speed up boarding, cut queues and eliminate physical contact during the Covid-19 crisis, and passports and tickets will only be necessary once customers reach their destination.

Privacy campaigners had questioned the need to introduce facial recognition cameras when travel on Eurostar already uses contactless technology.

Ilia Siatitsa, legal officer at Privacy International, said the level of intrusion of facial recognition technology is so high that the legality of its use should be questioned.

“Being efficient or quick for travelling [is] not sufficient justification for introducing such intrusive technology, particularly where there can be other alternatives,” she said.

iProov will process images to ensure the identity and “genuine presence” of the passenger. The technology aims to verify that the user is a real person and not a photo, video, mask or deepfake.
Andrew Bud, Founder and CEO at iProov, described the project a “world first”, and said the initiative has grown from its original aim to help “reduce travel congestion and keep passengers moving”, and is now going to help “keep people safe in a pandemic world through social distancing and contactless interaction”.

Ethical questions

Privacy International’s legal officer Ilia Siatitsa, said that “intrusive technologies” raise ethical and data protection questions. “Biometrics are a very sensitive category of data … We cannot change our facial characteristics, fingerprints, or our DNA.”

Facial recognition technologies by both police and private companies can have a "seismic impact" in the potential monitoring of individuals, she said. "With facial recognition, the level of intrusion is so high that the legality should be questioned to begin with."

Siatitsa said travel and the processing of identity documents are already virtually contactless. "You go, you scan your ticket, you pass the security check," she said. "It's difficult to see … the justification for rolling facial recognition when there is already quite an efficient process in place."

No need to 'fumble' with paper tickets

Bud said Eurostar's previous system involved "fumbling around with scraps of paper and barcodes".

Facial recognition technology is a secure and beneficial addition to public life. "The citizen knows that their face is to be verified, they consent to [it] and get personal benefit from being verified," said Bud.

Eurostar's strategy director Gareth Williams said that eliminating the need for passports through the use of biometric facial verification will "enhance passenger experience" and "offer a live illustration of how innovation can benefit the high-speed rail and international transport industries".

The initiative is part of a £9.4 million competition funded by the Department for Transport to advance rail travel and facilitate contactless journeys. On

Wednesday, the department offered iProov a £388,000 grant to finalise developments.

Dutch organisations address business email compromise fraud

Kim Loohuis

The FBI’s Internet Crime Complaint Center received nearly 24,000 reports of business email compromise (BEC) fraud last year, involving sums totalling more than $1.7bn worldwide. To tackle this highly damaging form of cyber crime – and other types of attack – in the Netherlands, the Dutch Public Prosecutor’s Office and the Hague Security Delta Office are working in a public-private partnership with banks, companies, governments and knowledge institutes.

The best-known case of BEC fraud – also known as CEO fraud – in the Netherlands concerned cinema chain Pathé. In 2018, criminals posed as directors at the company’s French head office and sent emails to its Dutch management requesting money to pay for a takeover abroad. The Dutch management received an urgent request not to tell anyone about the transactions in order to take the wind out of competitors’ sails.

Although Pathé’s Dutch management had their doubts about the request, they cooperated. After the first transaction, the fraudsters started asking for ever larger amounts and a total of €19.2m was taken. It was only when the Dutch management knocked on the door of their French parent company to explain there was too little money to transfer, that the CEO fraud became apparent.

The Netherlands' public-private partnership to tackle BEC fraud aims to map out how cyber criminals work to disrupt their business model and increase the chance of identifying the cyber criminals. Lodewijk van Zwieten, prosecutor of cyber crime at the Public Prosecutor's Office, said: "We are working with various partners to gain insight into the processes and modus operandi of cyber criminals. After all, the old-fashioned search for criminals does not always work effectively in the digital world.

"By gaining insight into the digital criminal business model, we can tackle the phenomenon. We have chosen to start with the cyber crime method that causes the most damage worldwide – BEC."

Although the FBI has reported global losses of $1.7bn resulting from BEC, actual losses are likely to be higher. Many companies do not report such attacks, which is why no reliable figures are available for the Netherlands.

"There is only limited reporting and the figures that are available say very little," said Van Zwieten. "But that is no reason to doubt the figures from the FBI and various security companies. We want to invest as much as possible to combat this cyber crime."

Once the cyber criminals' business model has been revealed, it is important to disrupt the processes effectively, said Van Zwieten. "The use of criminal law is not always effective or desirable in tackling this type of crime," he said. "But when such a criminal has a business model with dependencies – in the ordinary world, we call that a supply chain – then an approach can focus on that supply chain.

"We see that hardened criminals hide themselves very well, which makes it difficult to catch them, but if we disrupt their business model by focusing on the facilitating organisations, we have a better chance of getting close to them."

"What we are mapping out is the complete process that an average BEC criminal follows, from the moment he or she gets an idea, to the moment they put the money in their back pocket. We really put ourselves in the criminal's shoes and try to figure out what steps they have to go through and who and what they need.
"This way, you find out that criminals also need external expertise. They can get it from an above-ground market, such as hosting, or from an underground market, such as knowledge about money laundering. We map out this value chain within the partnership."

The group is currently developing a number of interventions to make it more difficult for cyber criminals to carry out their work. "By this, we mean interventions that make potential victims more resilient," said Van Zwieten. "For example, we are also working with banks to see how we can trace fraudulent transactions sooner."

Van Zwieten gave the example of a digital invoice, on which the account number is changed by a criminal. When a bank sees such a transaction, an alarm bell should go off because the account number differs from the one through which regular payments are made.

"This is how we actually try to erect all kinds of barriers for BEC criminals as quickly as possible," he said. "Things that make the criminal's processes not run so smoothly, so he or she stops or has to go to a lot more trouble. Criminals often don't want the latter, because then they have to step out of the shadows, increasing the chances of being caught."

Broader cooperation

The Netherlands' partnership also works with others inside and outside the EU, but for the time being, these partnerships depend on individual cases. "Our ambition is to work more structurally with a group of countries against cyber crime and BEC," said Van Zwieten. "It is valuable to share experience and knowledge about how cyber criminals operate and which interventions work effectively to disrupt business models. We have this ambition for BEC, but also for other phenomena, such as DDoS [distributed denial of service], ransomware and phishing.

“We also want to collaborate with the [Dutch employers’ organisation] VNO-NCW to determine how we can get the message to the right companies in the right way.”

Now that the Covid-19 crisis is forcing many companies’ employees to work from home, the Netherlands’ public prosecutor is expecting an increase in cyber crime. “We foresee an increase in digital attacks,” said Van Zwieten, “not only by cyber criminals, but also by young people who are obliged to sit at home, get bored and then seek their pleasure behind a keyboard.”

He pointed to the DDoS attack that recently hit Dutch meals-on-wheels organisation Thuisbezorgd. “To carry out such an attack, you don’t have to be a seasoned cyber criminal,” he said.

But the current crisis is also fertile ground for CEO fraud, Van Zwieten added. “People may not be surprised to suddenly receive an email from their boss asking them to transfer a large sum of money, otherwise the company will fall apart in this crisis.”

That is why the work of the Netherlands’ public-private partnership is so important, he said. “We want to demonstrate that this is a good way to deal with cyber crime and so make the Netherlands and Dutch companies a lot more unattractive to cyber criminals.”

EU judges GDPR an overall success, but changes still needed

Alex Scroxton, Security Editor

The European Union (EU) General Data Protection Regulation (GDPR) has been assessed as an overall success in terms of meeting expectations and objectives, but more time is needed to smooth out some early issues identified by stakeholders, according to a two-year progress report issued by Brussels.

The European Commission (EC) said it would be premature to draw definite conclusions as to the application of the GDPR, and to provide for proposals for any revisions, but said it had identified a number of areas where improvements could eventually be made.

It said that the GDPR had made EU citizens feel more empowered and aware of their enforceable rights and protections – according to the EU Fundamental Rights Agency, 69% of those aged over 16 have heard of the GDPR, and 71% have heard about their national data protection agency. In general, it said, people feel they can play an active role in controlling their data.

On the business side, the EC said that organisations felt that having one consistent set of rules to adhere to across the EU had been a benefit, as well as levelling the playing field when competing with organisations not based in the EU but operating there. Small to medium-sized enterprises (SMEs) tended to feel that many of the provisions of the GDPR had lowered the barriers to entry to data protection friendly services.

The GDPR is also contributing to fostering more trustworthy innovation through risk-based approaches and principles such as privacy by design – the EC noted its approach had been tested during the Covid-19 pandemic and shown to be successful, with principles-based rules supporting the development of tools to effectively combat and monitor the spread of the virus.

The EC also said that the EU's disparate data protection authorities (DPAs) had shown they could actively work together since the introduction of the GDPR, however it noted that that neither a dispute resolution nor an urgency procedure have yet been triggered under the regulations.

The EC made a number of suggestions for improvements around differences in national administrative procedures and how different EU member states interpret various concepts under the rules – the European Data Protection Board has already indicated that it will clarify procedural steps to help in this regard.

Going forward, it will act to make sure that national rules are better in line with the GDPR; that each member state can provide their DPAs with the needed resources; that DPAs are helped to develop more efficient working arrangements on the cooperation and consistency mechanisms; that the full toolbox available under the GDPR is uses to better apply the rules; and that the application of the GDPR to emerging technologies such as artificial intelligence (AI), blockchain, and the internet of things (IoT) is closely monitored.

Chris Harris, Europe, the Middle East and Africa (EMEA) technical director at Thales, said the EC was right to zero in on the need for clarification and to look at how the 27 different DPAs work together.

“Since [GDPR’s] inception, there has been murmurs about its effectiveness due to lack of clarity on compliance and fears around the resources and power each DPA has to track and investigate the number of breaches that occur in their country. This is something that should have been sorted from the start, and not something that we are still talking about two years later – four if you include the transition period,” he said.

“To be truly effective, the EU needs to give clearer instructions on how to be compliant that are consistent across each country, while giving local DPAs more resources to pursue heavy penalties against companies that are intentionally putting their customers’ data at risk.”

Tom De Cordier, a Brussels-based partner at law firm CMS, said that contrary to the EC’s view, the Covid-19 crisis had laid bare some of the problems inherent in the GDPR.

"Despite GDPR offering a high level of protection to citizens by default, the public trust in its effectiveness remains extraordinarily low – as demonstrated by the ongoing privacy debate surrounding contact-tracing apps and slow progress on introducing large scale initiatives that could help meaningfully curb the spread of the coronavirus," he said.

"More than ever, we need governments and tech companies working together to build trustworthy technology to tackle the biggest health crisis of the century and clearly communicate the regulations that surround it.

"Moving beyond the crisis, supporting innovation and emerging technologies such as 5G and IoT will be key in bringing new economic opportunities. Currently, Europe is working under ePrivacy laws from 2002, which don't easily interface with the GDPR and are in dire need of an update," said De Cordier.

Twitter contacts business users over data exposure

Alex Scroxton, Security Editor

Social media platform Twitter has begun contacting a number of business users in relation to a long-standing data security issue that may have seen their personal information exposed if a highly specific set of circumstances occurred.

Twitter told affected users that before 20 May 2020, if they viewed their billing information on ads.twitter.com or analytics.twitter.com, data including email addresses, phone numbers, the last four digits of credit card numbers, and billing addresses “may have” been stored in their browser’s cache.

Because most browsers generally store such data for a given period by default, if an affected user was using a shared computer, it would be possible for another user to access and view that data, the firm said in a disclosure email, a copy of which was seen by Computer Weekly.

“We’re very sorry this happened,” the organisation said in the email. “We recognise and appreciate the trust you place in us, and are committed to earning that trust every day.”

Twitter said that as of 20 May, the vulnerability has been fixed by updating the instructions Twitter sends to browser caches to prevent this from happening again.

The firm said it had no evidence that any billing information was compromised as a result of the vulnerability.

To exploit the vulnerability, an attacker would need physical access to the victim’s device, and would probably have to be known to the victim, so it is quite unlikely that any of the account data affected has been exfiltrated by cyber criminals.

Nevertheless, in a business context, there always exists an element of risk from malicious insiders, so Twitter said that if users do use a shared machine to access either their ads or analytics billing information, they should clear their browser caches when they log out, as a precaution.

At the time of publication, Twitter had not yet responded to a request for comment, so it is as yet unclear how many accounts may have been at risk of compromise, should the vulnerability have been exploited.

Martin Jartelius, chief security officer at Outpost24, agreed that the likelihood of compromise was slim. “This access has to be done on the computer on the same account as you used, or by a user with permissions to access the cached information,” he said.

"Using personal accounts when using computers, and not accessing personal accounts from shared systems such as in a library, are good practice. Accessing any account from a system you do not control, such as in the case of a library or other shared systems, already means the information could be accessed by the owner of that system if they monitor your activity."
Jartelius added: "The fact that Twitter is reaching out to their customers regarding this is a very strong statement regarding their focus on their customers' privacy and security."

Javvad Malik, security awareness advocate at KnowBe4, said: "This is a good proactive step taken by Twitter in notifying potentially impacted users. It appears as if this would only manifest as an issue in the event that a shared computer was used.

"It is worth users being mindful of what actions they perform on a shared device and should avoid logging onto accounts and making payments on shared or public devices unless absolutely necessary. If it does need to be done, they should ensure they are logged out of all accounts once they are done."

Getting more CW+ exclusive content

As a CW+ member, you have access to TechTarget’s entire portfolio of 140+ websites. CW+ access directs you to previously unavailable “platinum members-only resources” that are guaranteed to save you the time and effort of having to track such premium content down on your own, ultimately helping you to solve your toughest IT challenges more effectively—and faster—than ever before.

Take full advantage of your membership by visiting www.computerweekly.com/eproducts

Images; stock.adobe.com