Building a framework to meet the new financial landscape's security challenges

PSD2 and Banks

pwc

Introduction

The financial services industry is starting to treat Open Banking as a critically important, strategic topic that cannot be ignored due to the size of the opportunity and the potentially disruptive impact it could have on the landscape. This paper is a follow up to our paper 'The future of banking is open – how to seize the Open Banking opportunity'[1] and aims to help banks think through the security challenges related to the revised Payment Services Directive (PSD2), which came into law in January 2018.

Designed to drive innovation in the banking sector, PSD2 will enable the development of new financial products and services for the benefit of consumers and SMEs alike. Under PSD2, banks are now mandated to allow a regulated third party provider (with a consumer's consent) to secure access to a consumer's account information and/or request payments be made. This access will be enabled via open application programming interfaces (APIs), in line with Regulatory Technical Standards (RTS) that will govern the security of this access (RTS is likely to become applicable in September 2019).

With PSD2 having come into law earlier this year, the contours of this new financial landscape are starting to emerge.

There are 3 broad security challenges that banks need to consider:

1 Consumer awareness of PSD2 remains low

Media coverage of the new directive has largely focused on potential risks – fraud, data breaches and privacy implications have all been highlighted – rather than potential benefits of the new directive. Comparisons have been drawn with contactless payments: a slow start (in part owing to concerns over fraud) before rapid adoption amongst the general public. Today, contactless payments are firmly embedded in everyday life.[2] If PSD2 is to follow a similar trajectory, consumers will need to clearly see the benefits of the new directive. For this to happen, consumers will need to feel confident that their data will remain safe and secure in this new financial landscape.

2 Greater connectivity between banks, third parties and consumers can be expected

As one challenger bank told PwC recently, 'APIs are intrinsic to what we do.' This theme of greater connectivity applies to established banks too, as closer working with third parties to help develop digital solutions for customers (and internal applications) becomes the norm.

3 Banks still need to keep the data of their consumers safe and secure

Although PSD2 (and Open Banking in the UK) is premised on change and innovation, banks should not lose sight of the fact that they need to keep the data of their customers' safe and secure at all times. This tenet applies regardless of whether banks choose to fully embrace the new directive and the innovation it promises, or if they seek simply to meet minimum regulatory requirements.

Rather than waiting for the new financial landscape to take hold, banks should be building a framework now that will allow them to manage these security challenges in the round. This should be an evolution – not a revolution – of the existing framework that banks currently use to manage security threats.

This paper utilises the NIST[3] cyber security framework, as one of the most commonly used industry benchmarks, in order to structure and set out a framework to help banks think through how they might start to address the security challenges faced with PSD2.

[1] https://www.pwc.co.uk/industries/financial-services/insights/seize-open-banking-opportunity.html

[2] 'Open Banking – are consumers ready?' Ipsos MORI, November 2017 https://www.ipsos.com/ipsos-mori/en-uk/open-banking-are-consumers-ready

[3] https://csrc.nist.gov/publications/sp800

Building a framework

Identify

The first step that should be to taken is for banks to consider how PSD2 will extend the ecosystem in which they operate and the complex network of connected systems. It is no longer sufficient for a bank to map out the relationships it holds: customers and suppliers, peer banks, payment schemes etc. Banks now need to think in terms of the connections and infrastructure that support these relationships, infrastructure that is increasingly digital in nature. High profile cyber attacks have underlined the importance of thinking in terms of an ecosystem: *Operation Cloud Hopper*[4] last year highlighted a threat campaign that targeted IT Managed Service Providers (MSPs), allowing a threat actor potential access to MSPs and their clients on a global basis. This access was achieved not by targeting the clients themselves, but the connections to these clients.

In the context of PSD2, banks should be thinking of their ecosystem and considering the following factors:

[4] https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/operation-cloud-hopper.html

The new connections (the APIs) that will be established

Will these APIs extend the attack surface that needs to be protected (even if there is an existing relationship in place between the bank and the third party)? Is the API established with an authorised (under PSD2) third party, or could it be fraudulent in nature?

The data that an API will be able to access

Once a bank has mapped out a new or existing API, they should consider the data that may be accessed by the API, including customer bank account information, or payments information. The more valuable the data, the more attractive it will be to a (broader) range of threat actors.

The access the API should (and should not) have

Banks should consider the access that an API will provide a third party to the bank's systems. Will this access be an attractive target to threat actors? Banks should think beyond the access that should be provided by an API. In the event of compromise, could the API provide access to other assets, e.g. could an API connected to a customer facing website also provide access to any databases sitting behind the website?

The new entrants to the market

Banks should start to think about the new third party providers (TPPs) entering the market under PSD2. Even if a bank already holds a relationship with a TPP, this relationship is likely to change. TPPs will become more established and will offer more financial products and services to consumers. Indeed, even if PSD2 fails to revolutionise the consumer banking market, it seems likely that TPPs will play a part in the banking landscape.

Detect

As banks build a framework for managing the security challenges relating to PSD2 it is vital that taking a proactive approach to understanding security threats is factored in. As part of this **proactive approach** the following should be mapped out:

A baseline understanding of API activity

Customer-facing colleagues in banks should hold data that can be leveraged here. Data on which APIs are already in place, popular times for their usage, 'typical' volumes, and so on. This data can then be used by bank security functions to help identify patterns of activity outside the parameters of 'typical' usage, indicative of a potential attack, e.g. high volumes and sudden spikes in usage.

Existing threat scenarios

Given the emphasis on innovation behind PSD2 it is easy to forget that APIs are not new (in consumer banking or elsewhere). Banks can draw on their own experience and that of others in thinking through the most likely threat scenarios that may apply under PSD2. The OWASP 'Top Ten', for instance, is widely recognised as an authoritative source on potential threats relating to APIs. In addition, banks should consider engaging with developers and businesses outside the finance community to understand latest techniques, tools and processes used by threat actors targeting APIs.

The 'new' threat scenarios they face

Banks should not limit themselves to the existing threat scenarios in relation to third parties and APIs. Broader threat modelling should be encouraged, to think through the range of defensive strategies that should be employed to help protect consumers, their data and funds. As more innovative financial services and products are developed, this lateral thinking will become especially important.

What security testing will look like under PSD2

As new connections are formed with new and existing TPPs, banks will need to think through security testing in this context. Building on the threat modelling steps outlined above, banks should think about a broad set of functional, non-functional, bounds and vulnerability testing of any potential APIs to be established. Threat actors will not limit themselves, after all, to how an API 'should' be used if they find using it in another way provides them with the means to target a bank, their consumers and their data.

In addition banks will need to consider the speed with which they are asked to deploy an API against the 'normal' lifecycle of security use testing. Expectations of TPPS and that of consumers (over time) around the speed of deployment of a new API may not marry up to the typical testing practices of a bank. As part of the approach taken to testing, banks (in the UK at least) can familiarise themselves with the on-boarding and attestation process that the Open Banking directory will undertake (governed by the Competition and Markets Authority). Providing a TPP has been on-boarded by the Open Banking directory, banks will not be able to refuse this TPP access to the account payment information that the bank holds. This will provide a greater degree of regulation than exists today with regards to TPPs 'screen scraping' information from banks. Taking a proactive approach here will help banks to understand their risks and prioritise investment accordingly.

[5] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Protect

Banks need to think through the importance of **identity** in a financial landscape where greater connectivity to third parties and consumers will be increasingly common. Thinking through the concept of identity in this context will help banks take a more strategic approach to PSD2 and security, rather than focusing on individual connections and individual security risks. There are a number of themes that banks should consider here, including:

An opportunity for banks to help consumers

Banks can use PSD2 to kick-start (or perhaps continue) a conversation with consumers on personal data. As a starting point, PSD2 is predicated on the belief that personal data is valuable, and that it is owned by an individual. Banks can use PSD2 to reinforce existing messages to their consumers on the value of personal data and the need to keep it safe and secure.

There is also an opportunity for banks to take this conversation further. Consumers are aware that personal data is changing: a poll from 2017 found that almost 70% of those surveyed agreed that 'providing personal information is an increasing part of modern life.' Consumers' understanding of **how** their data is used (and shared) appears to be more limited: the same survey noted that only 8% of the UK public has a good understanding of how their information is made available to others.[6]

Banks can help to bring clarity to an area of today's digital world that consumers find confusing. Although the technical standards of PSD2 (RTS) are yet to be developed in detail they should provide a transparent and structured way for consumers to share their account information with TPPs. External drivers are also accelerating this trend – recent headlines have caused consumers to start to question in more detail how 'big tech' is using their data, including the levels of permission granted before data is shared across platforms and apps.

Banks can also start to have conversations with consumers about 'digital identity' – the multiple ways in which consumers use their identity across digital platforms in their daily lives, from banking to shopping and booking medical appointments. Consumers making use of the services offered by TPPs under PSD2 need to be aware of the security risks. Banks can take the opportunity to remind consumers that they should only share their personal data with parties they trust, in a manner that they feel is secure.

An opportunity for banks to think about digital identity

PSD2 gives banks the opportunity to think more fundamentally about how they manage identity in today's digital world. Banks should recognise that under PSD2 consumers will increasingly use their banking identity to authenticate against other services and channels. At a simple level this already happens today, for instance using a bank statement as proof of address when buying a new mobile phone.

There may be a business opportunity for banks here; Offering a digital (banking) identity service to consumers that allows them to access a growing range of services and channels. At the very least, banks have an opportunity to consider how identity under PSD2 fits into their wider business model and the existing, different authentication methods used by consumers to access banking channels and products today (e.g. online banking versus mobile banking).

Thinking through identity and authentication under PSD2

Alongside the focus on furthering innovation and competition, PSD2 has an explicit aim of 'increasing the level of security of electronic payments.' In this regard, the RTS defines the requirements for strong customer authentication, which is to be used when a consumer accesses a payment account, as well as for making payments online. Further detail on strong customer authentication and how it applies in the context of PSD2 are set out by the European Banking Authority.[7]

Banks will be aware of their regulatory obligations under PSD2, including the specifications outlined in RTS. However, banks also need to think through the relationship between the General Data Protection Regulation (GDPR) and PSD2, with the requirements under GDPR meaning a consumer has to give their consent before their data is held and shared by an organisation.

In building a framework that helps manage the security challenges related to PSD2, banks should think more broadly than 'just' the regulatory requirements. Threat actors for one will pay little attention to any new regulatory requirements and focus instead on the best way to attack banks and their customers (including both their data and funds). Banks need to consider the broader security challenges that arise from PSD2 than just ensuring compliance with RTS and attendant requirements.

[5] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[6] http://www.comresglobal.com/polls/ukcloud-personal-data-survey/

Respond and Recover

As banks start to think through the security challenges related to PSD2, they can fall back on an existing approach: **defence in depth**. Banks have long recognised that while protecting the perimeter of their organisation is important, it is not the only step they need to take to protect themselves from security threats. Building a set of multi-layered controls will help banks to better respond to the security challenges posed by PSD2.

The design and development of these controls should be based on the elements outlined in the above framework:

- Thinking about threats in relation to the ecosystem in which the bank operates
- Taking a proactive approach to security risks, undertaking a broad set of threat modelling
- Using this threat modelling to inform security testing
- Thinking through identity both in the context of PSD2 and in terms of current approaches to authentication
- Recognising the regulatory requirements of PSD2, including on strong customer authentication, but also thinking more broadly on authentication

'Defence in depth' in the context of PSD2 should mean thinking about security across all stages of the development process, from the design stage to the implementation stage and beyond. APIs will clearly be at the centre of this 'defence in depth' thinking, given their centrality to PSD2 and Open Banking.

However, banks will be remiss if they think about controls in purely technical terms. Security policies, for instance, should be reviewed to ensure that the growing importance of connectivity to TPPs is recognised. Banks should think through the agile processes required to meet consumer demand that may flow from PSD2 and what this will mean for existing approaches to security, for instance current governance models around establishing connectivity to third parties.

Incident management procedures, policies and related standards will need to be updated too in order to reflect the growing connectivity with TPPs under PSD2. Existing playbooks regarding a security incident at a TPP will help banks think through the approaches they will need to take in the event that a TPP is breached that under the new directive has access to consumer accounts. Preparedness will be key with simple steps such as having relevant contact details at hand and having protocols for sharing intelligence such as indicators of compromise will need to be thought through.

[7] https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/technic-standards-on-the-eba-register-under-psd2

Conclusion

It has been almost a year since Open Banking came into law. It is time for banks to not only take stock of how they have managed the challenges and opportunities to date, but also ensure they are planning effectively for the future. In particular, security teams need to be clear on the strategic direction that the bank as a whole is taking on Open Banking before mapping out how they can best support this strategy.

As the recent PwC report on Open Banking[8] notes 'Open Banking is here and will transform the way we are able to pay for goods and services and manage our finances. Open Banking creates a significant market opportunity and potential to disrupt the financial services landscape.'

Security teams now need to be working with their colleagues in the front line teams, including the technology team, any third party or supplier teams, to build out a strategy which answers some of the key points set out in our framework above.

- How will PSD2 extend my eco-system and what impact will this have? Including the connections established, the data that will be accessible, the access of APIS and any new entrants to the market
- How can we get on the front foot and take a more pro-active security approach? Considering the importance of a true understanding of threats and how security testing will be approached
- What does this mean for identity? Considering protecting consumers, digital identity and the importance of authentication
- How do we continue our 'defence in depth' approach? How does PSD2 impact security across all stages of the development process?

[8] https://www.pwc.co.uk/industries/financial-services/insights/seize-open-banking-opportunity.html

Intelligent Digital

At PwC, we are harnessing the power of Intelligent Digital, helping our clients to rethink their futures and reshape their own world. We are using business understanding, innovation in technology and human insight to help solve important problems, meet human needs and make a difference to society.

Helping our clients to understand the bigger picture of where their compliance operations, practices and controls fit into the regulatory landscape, and how they can be streamlined and improved to better safeguard them from risk, lies at the heart of PwC's support in the Compliance function.

Our teams help to build more simple, universal and integrated frameworks that deliver a clear understanding of compliance risk for our partners. Techniques and practices including culture and behavioural assessment, compliance programme remediation and third-party compliance programme development all stem from our commitment to the Intelligent Digital philosophy.

pwc.co.uk/intelligentdigital
#IntelligentDigital

pwc.co.uk

181024-150026-KM-OS