Anatomy of a Business Email Compromise Attack

30th November 2018

Version: 1.0

Table of Contents

Introduction

With the ever-increasing adoption of cloud-based email solutions such as Microsoft's Office 365, the attack surface for corporate email systems has expanded. With this comes an increased opportunity for malicious threat actors to target end users and exploit weak business processes to gain access to sensitive data and conduct fraud.

In this paper we will take a look at Business email compromise (BEC): what it is, how it can impact your organisation and more importantly, what you can do to reduce the likelihood that you will suffer from a breach.

What is BEC?

Business email compromise refers to the act of gaining unauthorised access to an individual's email account for the purpose of conducting financial fraud. While the attacker's main priority will typically be to use the account to steal funds from a company, the malicious threat actor will likely also attempt to exfiltrate sensitive data from the hacked mailbox and then use the same account to target others, with the aim of conducting repeat attacks and continuing to generate illicit profits.

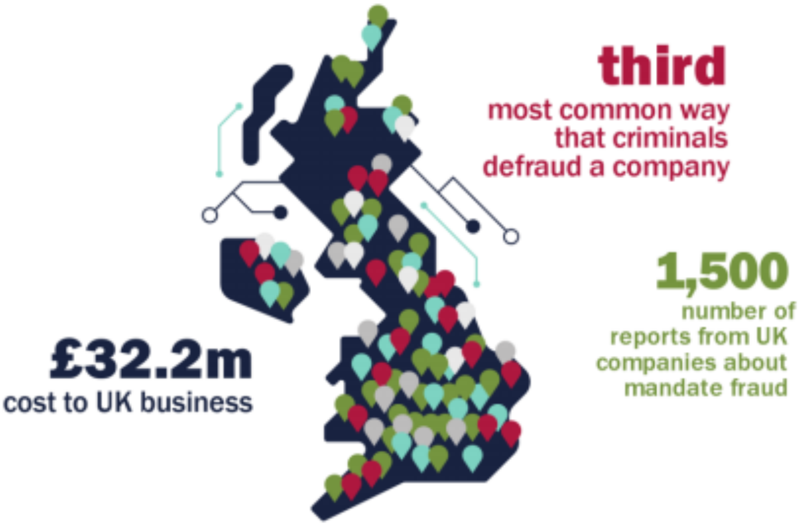
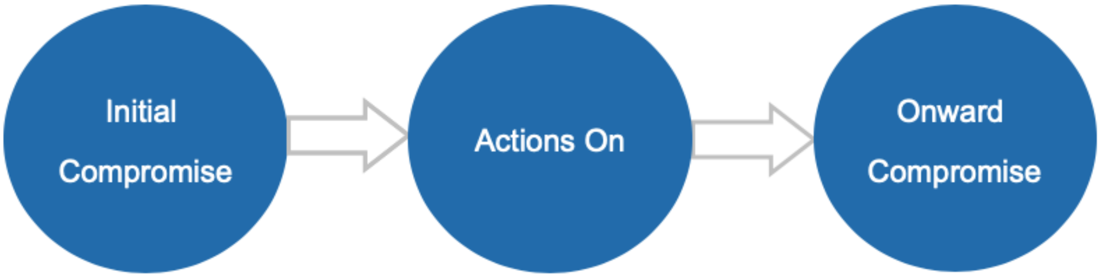

third
most common way that criminals defraud a company
1,500
number of reports from UK companies about mandate fraud
£32.2m
cost to UK business

Figure 1 - The cyber threat to UK businesses 2017-18 (NCSC)

Earlier this year, the UK's National Cyber Security Centre (NCSC) reported that BEC attacks cost UK businesses £32 million and the FBI warned that the total financial loss globally due to BEC attacks is at least $12.5 billion. In September 2018, the EU's law enforcement intelligence agency Europol advised that fraudsters operating out of West Africa who previously ran 419 scams are increasingly running BEC attacks instead. Given this switch, all organizations should expect to see BEC attacks escalate in the immediate future.

Anatomy of a BEC Attack

At a high level, the following three stages comprise a successful BEC attack methodology, as employed by malicious threat actors:



Here's a more in-depth look at each stage of a BEC attack campaign.

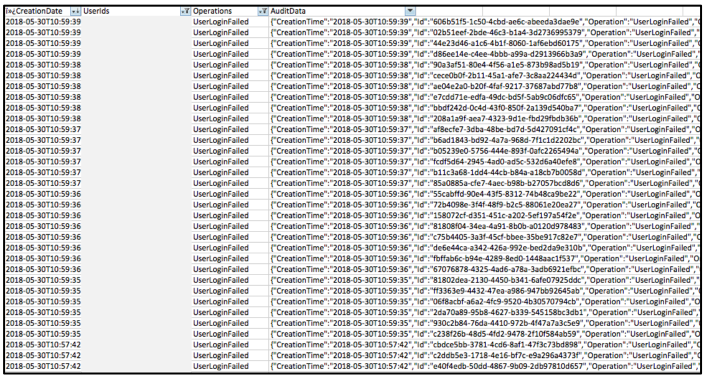
Stage 1: Initial Compromise

Attackers continue to spoof the email address of the CFO or CEO, or more generally to pretend to be a senior manager who has the ability to order wire transfers. In comparison to these types of 'CEO fraud' attacks, BEC attacks typically focus more on gaining access to a legitimate email account and thereby 'becoming' the user who is sending the emails, rather than simply trying to spoof the account.

To achieve this, malicious threat actors have a simple imperative: They must gain access to corporate email accounts. There are a number of techniques they can employ, but we regularly see two approaches via our incident response investigations: Brute-force password attacks, and phishing-based attacks that try to entice the end user to disclose their username and password.

Brute Force Attacks

By default, cloud-based solutions such as Office 365 do not protect end users from suitably timed and distributed password-guessing-based attacks that use brute force. These attacks often use slow-based timing, combined with distributed source IP addresses to avoid any throttling or blacklisting defences, and target email addresses with weak passwords. Successful identification of a valid username and password combination can then provide the attacker with direct access to that mailbox and associated infrastructure, such as a group mailbox and shared files.

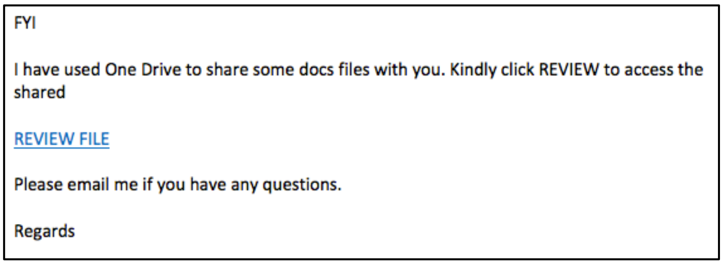


ï»¿CreationDate	UserIds	Operations	AuditData
2018-05-30T10:59:39		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:39","Id":"606b51f5-1c50-4cbd-ae6c-abeeda3dae9e","Operation":"UserLoginFailed","
2018-05-30T10:59:39		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:39","Id":"02b51eef-2bde-46c3-b1a4-3d2736995379","Operation":"UserLoginFailed","
2018-05-30T10:59:39		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:39","Id":"44e23d46-a1c6-4b1f-8060-1af6ebd60175","Operation":"UserLoginFailed","
2018-05-30T10:59:39		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:39","Id":"d86ee14e-c4ee-4bbb-a99a-d2913966b3a9","Operation":"UserLoginFailed","
2018-05-30T10:59:38		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:38","Id":"90a3af51-80e4-4f56-a1e5-873b98ad5b19","Operation":"UserLoginFailed","
2018-05-30T10:59:38		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:38","Id":"cece0b0f-2b11-45a1-afe7-3c8aa224434d","Operation":"UserLoginFailed","
2018-05-30T10:59:38		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:38","Id":"ae04e2a0-b20f-4faf-9217-37687abd77b8","Operation":"UserLoginFailed","
2018-05-30T10:59:38		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:38","Id":"e7cdd71e-edfa-49dc-bd5f-5ab9c06dfc65","Operation":"UserLoginFailed","
2018-05-30T10:59:38		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:38","Id":"bbdf242d-0c4d-43f0-850f-2a139d540ba7","Operation":"UserLoginFailed","
2018-05-30T10:59:38		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:38","Id":"208a1a9f-aea7-4323-9d1e-fbd29fbdb36b","Operation":"UserLoginFailed","
2018-05-30T10:59:37		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:37","Id":"af8ecfe7-3dba-48be-bd7d-5d427091cf4c","Operation":"UserLoginFailed","
2018-05-30T10:59:37		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:37","Id":"b6ad1843-bd92-4a7a-968d-7f1c1d2202bc","Operation":"UserLoginFailed","
2018-05-30T10:59:37		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:37","Id":"b05239e0-5756-444e-893f-0afc2265494a","Operation":"UserLoginFailed","
2018-05-30T10:59:37		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:37","Id":"fcdf5d64-2945-4ad0-ad5c-532d6a40efe8","Operation":"UserLoginFailed","
2018-05-30T10:59:37		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:37","Id":"b11c3a68-1dd4-44cb-b84a-a18cb7b0058d","Operation":"UserLoginFailed","
2018-05-30T10:59:37		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:37","Id":"85a0885a-cfe7-4aec-b98b-b27057bcd8d6","Operation":"UserLoginFailed","
2018-05-30T10:59:36		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:36","Id":"55cabffd-90e4-43f5-8312-74b48ca9be22","Operation":"UserLoginFailed","
2018-05-30T10:59:36		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:36","Id":"72b4098e-3f4f-48f9-b2c5-88061e20ea27","Operation":"UserLoginFailed","
2018-05-30T10:59:36		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:36","Id":"158072cf-d351-451c-a202-5ef197a54f2e","Operation":"UserLoginFailed","
2018-05-30T10:59:36		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:36","Id":"81808f04-34ea-4a91-8b0b-a0120d978483","Operation":"UserLoginFailed","
2018-05-30T10:59:36		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:36","Id":"c75b4405-3a3f-45cf-bbee-35be917c82e7","Operation":"UserLoginFailed","
2018-05-30T10:59:36		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:36","Id":"de6e44ca-a342-426a-992e-bed2da9e310b","Operation":"UserLoginFailed","
2018-05-30T10:59:36		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:36","Id":"fbffab6c-b94e-4289-8ed0-1448aac1f537","Operation":"UserLoginFailed","
2018-05-30T10:59:36		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:36","Id":"67076878-4325-4ad6-a78a-3adb6921efbc","Operation":"UserLoginFailed","
2018-05-30T10:59:35		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:35","Id":"81802dea-2130-4450-b341-6afe07925ddc","Operation":"UserLoginFailed","
2018-05-30T10:59:35		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:35","Id":"ff3363e9-4432-47ea-a986-947bb92645ab","Operation":"UserLoginFailed","
2018-05-30T10:59:35		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:35","Id":"06f8acbf-a6a2-4fc9-9520-4b30570794cb","Operation":"UserLoginFailed","
2018-05-30T10:59:35		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:35","Id":"2da70a89-95b8-4627-b339-545158bc3db1","Operation":"UserLoginFailed","
2018-05-30T10:59:35		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:35","Id":"930c2b84-76da-4410-972b-4f47a7a3c5e9","Operation":"UserLoginFailed","
2018-05-30T10:59:35		UserLoginFailed	{"CreationTime":"2018-05-30T10:59:35","Id":"c238f26b-48d5-4fd2-9478-2f10f584ab59","Operation":"UserLoginFailed","
2018-05-30T10:57:42		UserLoginFailed	{"CreationTime":"2018-05-30T10:57:42","Id":"cbdce5bb-3781-4cd6-8af1-47f3c73bd898","Operation":"UserLoginFailed","
2018-05-30T10:57:42		UserLoginFailed	{"CreationTime":"2018-05-30T10:57:42","Id":"c2ddb5e3-1718-4e16-bf7c-e9a296a4373f","Operation":"UserLoginFailed","
2018-05-30T10:57:42		UserLoginFailed	{"CreationTime":"2018-05-30T10:57:42","Id":"e40f4edb-50dd-4867-9b09-2db97810d657","Operation":"UserLoginFailed","

Figure 2 - Audit log showing a brute force password attack

Phishing Attacks

We have also seen increased activity by attackers who use phishing emails to entice end users into disclosing their username and password directly to the malicious threat actor. Often the phishing email will come from a previously compromised account. Because the sender is in the recipient's contact list, this often means that the recipient -- in reality, the target -- trusts what the email has to say more than if it came from an unknown user.



FYI

I have used One Drive to share some docs files with you. Kindly click REVIEW to access the shared

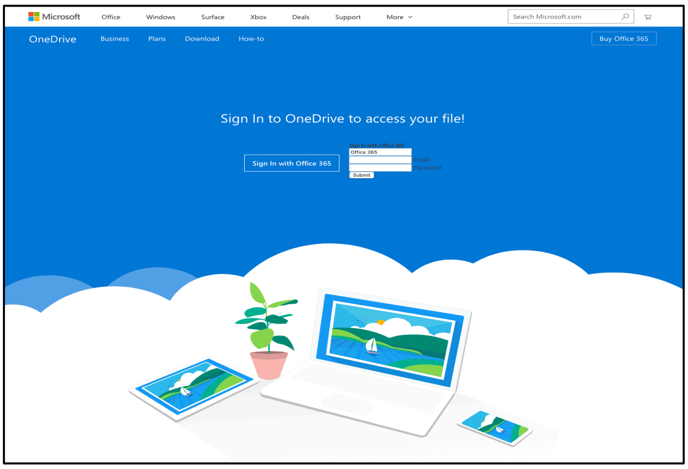
REVIEW FILE

Please email me if you have any questions.

Regards

Figure 3 - Example of a real phishing email

While specific approaches vary, in general, attackers try to entice a user into following a link -- often to a shared folder -- for the stated purpose of retrieving a work-related document. The link will take the user to a compromised website that pretends to be an online folder. In the case of Office 365, this will appear to be a legitimate OneDrive storage site. The site will be properly branded, present an official-looking login page and request that the user enter their credentials. Whatever information that gets entered then gets directly routed to the malicious threat actor, who can use it to try and gain access to the victim's account.



Sign In to OneDrive to access your file!

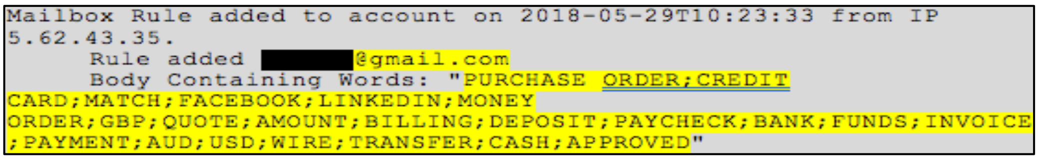
Sign in with Office 365
Office 365
Email
Password

Figure 4 - Example of a real O365 phishing site

Stage 2: Actions On

Once the first stage of gaining access has been completed, the malicious threat actor then progresses to trying to understand what type of information can be extracted from the account. Often an attacker's very first activity will be to set up a mail-forwarding rule to match specific keywords and automatically send them to an externally hosted email account under the control of the malicious threat actor. The keywords focus on extracting financially related data, but interestingly we have also seen keyword matching for personal information tied Facebook and LinkedIn accounts.

In one recent investigation, we identified a mail-forwarding rule that contained 22 keywords to be matched, and which resulted in more than 40 emails being exfiltrated within the first 48 hours of the compromise.



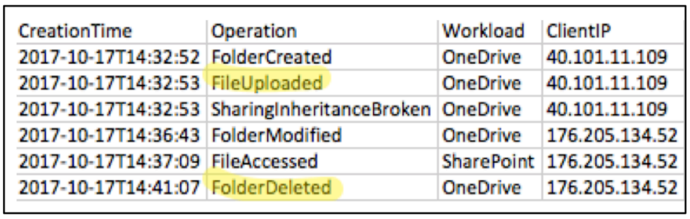
```
Mailbox Rule added to account on 2018-05-29T10:23:33 from IP
5.62.43.35.
     Rule added [redacted]@gmail.com
     Body Containing Words: "PURCHASE ORDER;CREDIT
CARD;MATCH;FACEBOOK;LINKEDIN;MONEY
ORDER;GBP;QUOTE;AMOUNT;BILLING;DEPOSIT;PAYCHECK;BANK;FUNDS;INVOICE
;PAYMENT;AUD;USD;WIRE;TRANSFER;CASH;APPROVED"
```

Figure 5 - Use of Mailbox rules to exfiltrate data

Stage 3: Financial Fraud

Once an attacker flags an account as being a likely vehicle for conducting financial fraud against the mailbox owner's organisation, the threat actor will then attempt to undertake such activity. During this phase, the threat actor will mimic the language of the end user and use the organisation's own internal approval processes to convince the relevant financial team to remit payments to an external, compromised bank account.

To hide their trail, malicious threat actors typically use mailbox rules to delete any incriminating emails they send -- hiding them from the legitimate user -- and oftentimes will rely on file-sharing solutions such as OneDrive to exfiltrate interesting-looking documents from the target's environment.



CreationTime	Operation	Workload	ClientIP
2017-10-17T14:32:52	FolderCreated	OneDrive	40.101.11.109
2017-10-17T14:32:53	FileUploaded	OneDrive	40.101.11.109
2017-10-17T14:32:53	SharingInheritanceBroken	OneDrive	40.101.11.109
2017-10-17T14:36:43	FolderModified	OneDrive	176.205.134.52
2017-10-17T14:37:09	FileAccessed	SharePoint	176.205.134.52
2017-10-17T14:41:07	FolderDeleted	OneDrive	176.205.134.52

Figure 6 - Example of data exfiltrated through OneDrive

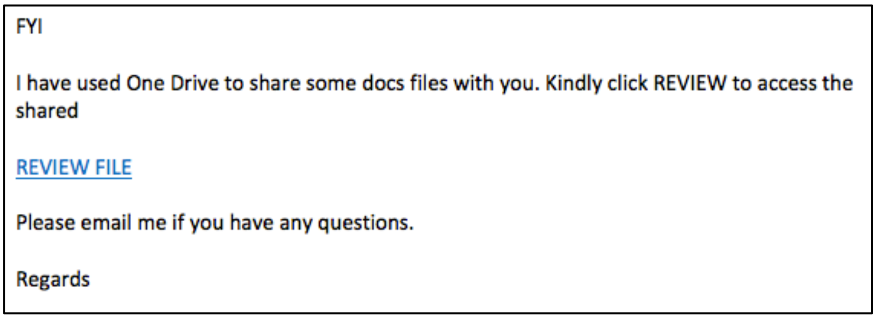
All of this activity is focused on keeping a low profile, to better ensure that attackers maintain access and increase their opportunity to repeat the scam and keep extracting funds until victims catch on.

During a recent breach, for example, an organisation lost £140,000 due to such an attack, which included four separate theft periods, spanning three months of sustained compromise.

Bonus Stage: Onward Compromise

At the point where the malicious threat actor is no longer able to commit fraud, or if the mailbox cannot support such activity, their focus typically shifts to using the compromised account to target others outside of the initially targeted organisation. This is often achieved by sending a phishing-based email to everyone on the user's email contact list, and repeating the entire attack against from stage one (the initial compromise phase) against every new target. Again and again with cybercrime, malicious threat actors prioritize the path of least resistance or effort, and we regularly see them reuse their same phishing templates over and over again.

Indeed, in one of our recent incident investigations, the email template that was used to entice the initial email accountholder into disclosing their username and password was then reused to target all contacts of that individual. And attackers did successfully gain access to other some of those follow-on targets' mailboxes.



FYI

I have used One Drive to share some docs files with you. Kindly click REVIEW to access the shared

REVIEW FILE

Please email me if you have any questions.

Regards

Figure 7 - Reuse of existing template

Mitigation

Ideally, organisations should look to reduce the likelihood of a compromise and therefore avoid having to react to an incident of this nature.

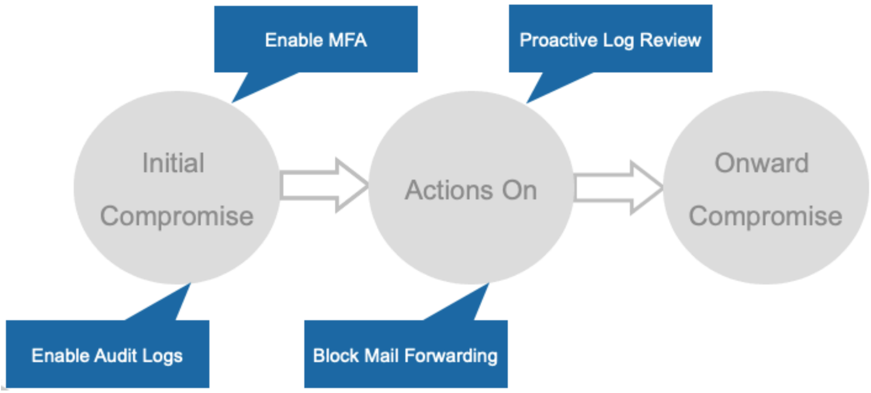


Figure 8 - Key mitigation

The best, first step for doing so is to implement multi-factor authentication (MFA). Doing so will mitigate the most common brute-force attacks and add an additional lay of complexity that any malicious threat actor would have to overcome after they tricked a target into divulging their email account password via a phishing attack.

Secondly, ensure that audit logs are enabled and retained for future use as part of any incident investigation. It is worth noting that within the Office 365 ecosystem, audit logs are only available for the default 90-day period. After this, they are no longer retained. Accordingly, organisations should take steps to routinely download and retain logs in the event that they are required by investigators.

In the event of an account compromise, the next step in mitigation should be to immediately block all mail-forwarding rules that try to move emails outside of an organisation's domain. As noted, attackers' first action will typically be to set a mail-forwarding rule designed to harvest potentially interesting emails and route them to an externally hosted email account, where attackers can review them. Setting a block will stop attackers' intelligence-gathering efforts as well as alert the organisation whenever it gets attempted.

If for operational reasons setting a mail-forwarding block is not possible, then consider setting an alert for the creation of any mail-forward rules, and proactively review these alerts as they get generated.

Also, it is essential to proactively review the environment for existing mail rules, especially because any changes may not arrest hackers' activities. If a new account password or MFA get applied to a previously compromised account, for example, existing rules will maintain persistence within the ecosystem and result in the continuation of emails being exfiltrated from the domain.

From an information security standpoint, the above is only a starting point. There are many more mitigating controls that can be implemented to provide a more robust approach to protecting environments, and specific control areas should be adopted to achieve a balanced approach to security. A balanced approach will provide additional protection against account breaches, elevation of privileges or data exfiltration types of attacks, covering not only the basic controls required but also a number of controls that effect a more "defence in depth" approach. Within the Office 365 ecosystem additional control areas should include generating weekly reports of suspicious sign-ins, including:

- **Failures:** Signs-ins after multiple failures
- **Unknowns:** Sign-ins from unknown sources
- **Geographies:** Sign-ins from multiple geographies

Combine these efforts with ongoing, proactive use of all available audit data, which can be invaluable not only to identify ongoing breaches, but also to immediately spot targeted attacks against specific users or against weak internal business practices, both of which increase the risk that an attacker can find a way in, leading to loss of data and in many cases, also money.

About 7 Elements

7 Elements is an independent and passionate security consultancy dedicated to working with our clients to help them secure their organisations. We provide expertise in the field of technical information assurance.

As a trusted partner to our clients we work to help effectively assess threats, identify security weaknesses and implement security resiliency to protect their business objectives. Key to this approach is working in close partnership with our customers. This builds long term relationships that enable tailored security approaches to be implemented that meet the organisation's business objectives.

Our knowledge is based on the successful delivery of security assessments for more than eight years. Our engagements range from single day reviews of firewall rules to long term global engagements. Our approaches have ranged from incident response to tailored security improvement packages of work, and from forensic investigations to assessments of the physical security of data centres. We have extensive knowledge and experience in the testing of critical and highly sensitive networks, from large global financials to protectively marked government networks.

At 7 Elements our approach to security testing is based on manual penetration testing techniques and goes further than simple vulnerability scanning. This approach, combined with our technical knowledge, ensures a deeper level of assurance and delivers pragmatic and tailored advice that is specific to the environment under test.

7 Elements
Independent information security consultancy

Twitter: @7Elements
Web: www.7elements.co.uk