AXIANS REDTOO

GDPR – Current IT Monitoring Trends and Capabilities

Lawrence Kwolek

08.11.2017

GENERAL OUTLINE

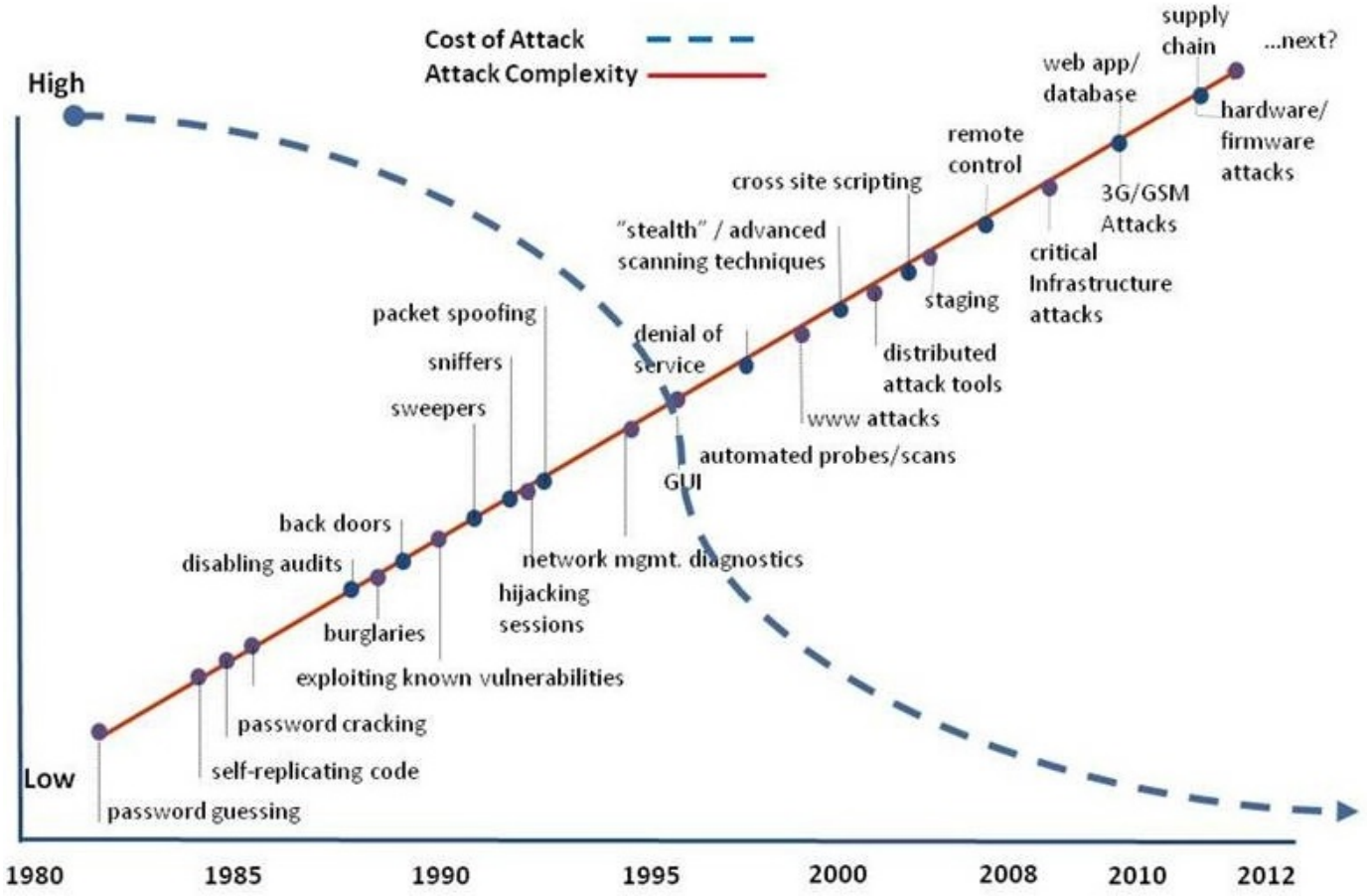
- The changing threats that are driving increased monitoring
- Understanding the current threats
- Anatomy of a cyber attack
- How monitoring is used to combat the threat?
- What is monitored?

The new face of hacking

THE INCREASING THREAT IS DRIVING GREATER MONITORING

Diminishing Attack Costs & Increasing Complexity

- Increased network complexity & dependence means more attacks succeed with high payoffs.
- Technology advances mean lower cost for a successful attack



COMMON ATTACK METHODS

- Malware
- Phishing
- SQL Injection Attack
- Cross Site Scripting (XSS)
- Denial of Service (DoS)
- Session Hijacking & Man-in-the-Middle Attacks
- Credential Reuse
- Social Engineering

When a criminal is trying to hack an organization, they won't re-invent the wheel unless they absolutely have to: They'll draw upon a common arsenal of attacks that are known to be highly effective.

Hackers are looking to exploit vulnerabilities to gain access to valuable data. Security experts are constantly trying to eliminated these threats.

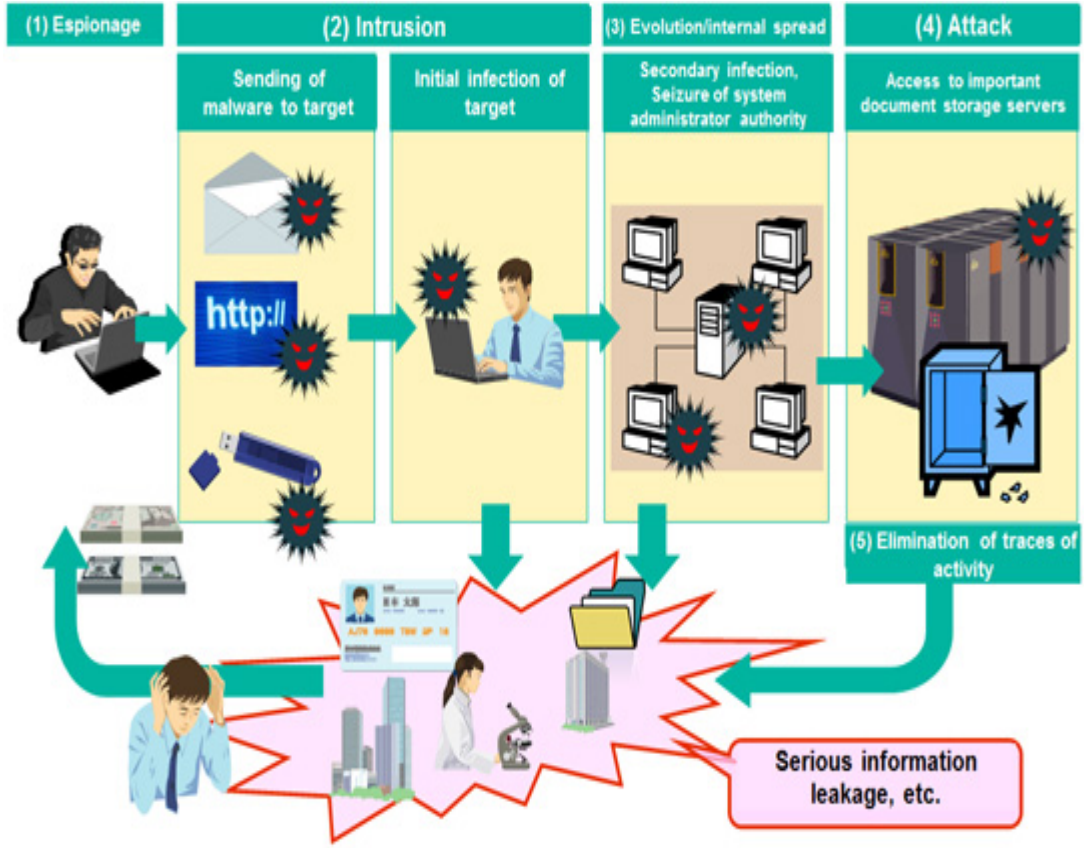
Whether you're trying to make sense of the latest data breach headline in the news or analyzing an incident in your own organization, it helps to understand the different ways an attacker might try to cause harm.

Here’s an overview of some of the most common types of attacks seen today.

OVERVIEW OF METHOD USED IN TARGETED CYBER ATTACKS (TYPICAL)

Targeted attacks are becoming increasingly sophisticated as they go through different stages:

1. Espionage
2. Intrusion
3. Internal spread
4. Attack
5. Elimination of traces of activity



MONITORING: WHO IS DOING WHAT, WHERE, WHEN?

Just a few of the current technologies that monitor, collect and control users

SIEM - Security Information and Event Management

- ***Collects and analyses user's activity and computer logs – can be on anything***
- A SIEM system collects data into a central repository for trend analysis and provides automated reporting for compliance and centralized reporting

Data End Point Protection

- ***Collects and analyses user's activity and computer logs - on clients***
- Antivirus, anti-spyware, personal firewall, application control and other styles of host intrusion prevention (for example, behavioral blocking) capabilities into a single and cohesive solution

Data Leakage Protection

- ***Labels data and tracks who accesses and transfers the data - on clients servers storage***
- Controls who can access data, even from unmanaged locations or devices, defines what level of access a user has using digital rights management technology, monitors user access to sensitive data to identify risky behavior or security compromise, and cam revoke access to users, effectively digitally shredding a document

MONITORING: WHO IS DOING WHAT, WHERE, WHEN?

Just a few of the current technologies that monitor, collect and control users

- **Identity Access Management (IAM) System & Privileged Elevation Delegation Management (PEDM)**
  - ***Controls access, collects and analyses user's activity and computer logs***
  - IAM technology can be used to initiate, capture, record and manage user identities and their related access permissions in an automated fashion
- **Web Content Filtering and Monitoring**
  - ***Controls, collects and analyses user's internet activity and reports noncompliance***
  - the use of a program to screen and exclude from access or availability Web pages or e-mail that is deemed objectionable
- **Anomalous Behavior Monitoring**
  - ***Collects and analyses user's activity and computer logs, "flags suspicious activity"***
  - Automated anomaly detection methods to detect possible anomalous behavior determined by malfunctions or external attacks

THANK YOU FOR YOUR ATTENTION

BACKUPS

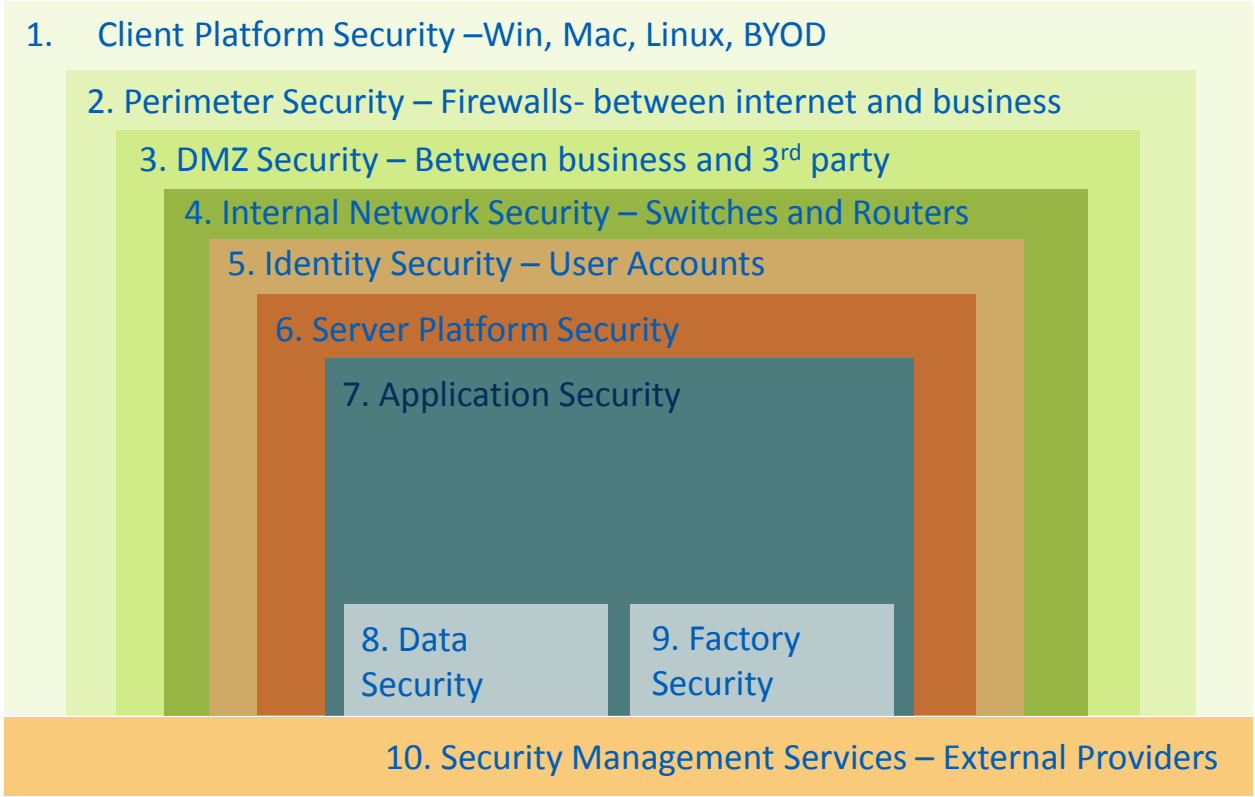
IT SECURITY MONITORING SYSTEMS

There are three ways that monitoring systems are generally divided:

1. Where the data is located, stored or transmitted?
    1. This refers to the Security architecture layer –
    2. Is the data on a hard drive? *Data at Rest*
    3. Is the data being transferred over the network? *Data In Motion*
    4. Is the data on an inactive backup system? *Data in Storage*
2. What form or state is the data in, what is it's encoding?
    1. This refers to the OSI Layer that the data is currently being transmitted or encapsulated in and Relates to *Protocols*
    2. *Protocols are simply a way of defining a common structure for data*
3. What *actions or processes* are occurring? Are they considered safe, unsafe or unknown?
    1. This can be on individual computing devices or data in motion

WHERE AND WHAT IS MONITORED?

Monitoring can occur on any layer and on any protocol



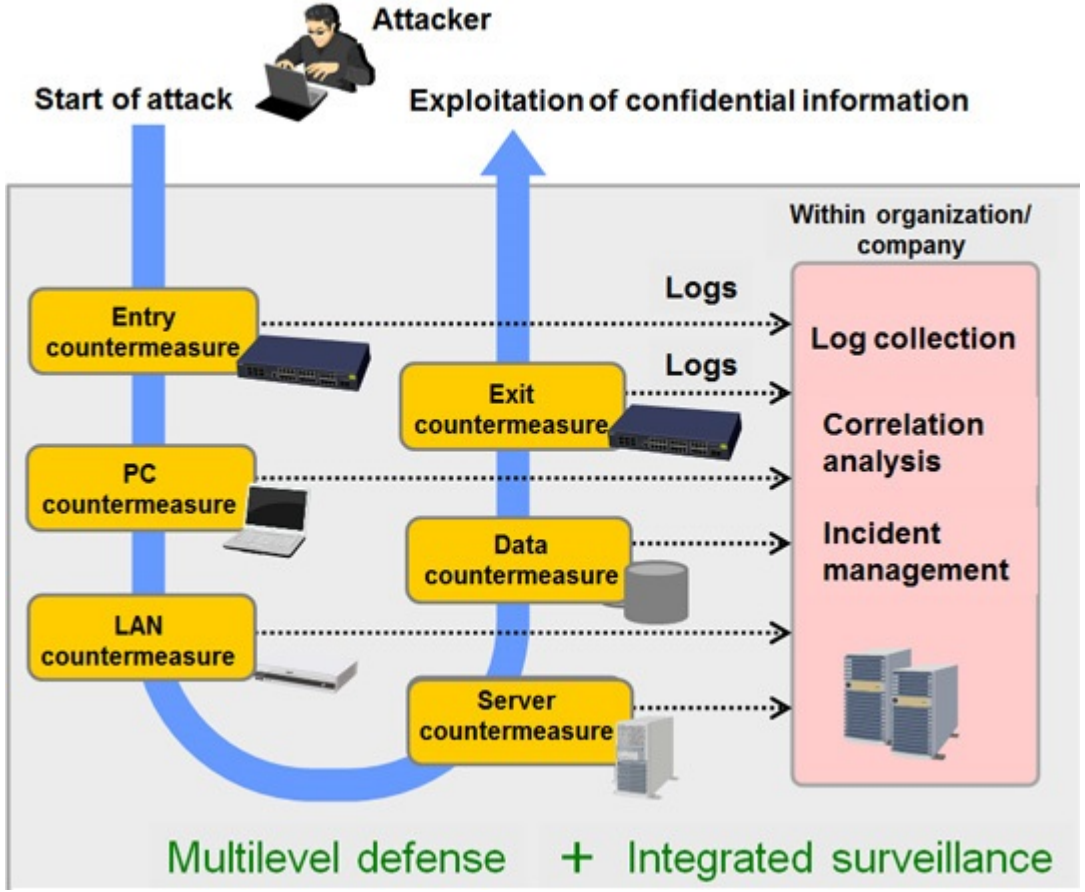
OSI Model	Protocols
Application Layer	DNS, DHCP, FTP, HTTPS, IMAP, LDAP, NTP, POP3, RTP, RTSP, SSH, SIP, SMTP, SNMP, Telnet,TFTP
Presentation Layer	JPEG, MIDI, MPEG, PICT, TIFF
Session Layer	Netbios, NFS, PAP, SCP, SQL, ZIP
Transport Layer	TCP, UDP
Network Layer	ICMP, IGMP, Ipsec, IPv4, IPb6, IPX, RIP
Data Link Layer	ARP, ATM, CDP, FDDI, Frame Relay, HDLC, MPLS, PPP, STP, Token Ring
Physical Layer	Bluetooth, Ethernet, OSI, ISDN, 802.11, Wi-Fi

SOLUTIONS TO STOP TARGETED ATTACKS

Four countermeasures against targeted attacks

1. Entry counter-measure
2. Exit counter-measure
3. Counter-measure against information leaks
4. Status visualization

Main take away –
All fours steps involve monitoring systems!



JUST A LITTLE TECH..... THE RISE OF THE MACHINES

- Current centralized IT security monitoring and analysis systems arose to more easily combat the growing risk of data loss and intrusion that is increasing exponentially.
- There are more devices connected to the internet than ever before. This is music to a hacker's ears, as they make good use of machines like printers and cameras which were never designed to ward off sophisticated invasions. It's led companies and individuals alike to rethink how safe their networks are.
- As the amount of these incidents rises, so does the way we need to classify the dangers they pose to businesses and consumers alike.
- Three of the most common terms thrown around when discussing cyber risks are vulnerabilities, exploits, and threats.
- To understand attack vectors, a little technical understanding is needed....

cyber risks are defined by vulnerabilities, exploits, and threats.

TYPES OF COMPUTER ATTACKS

MALWARE

- If you've ever seen an antivirus alert pop up on your screen, or if you've mistakenly clicked a malicious email attachment, then you've had a close call with malware. Attackers love to use malware to gain a foothold in users' computers—and, consequently, the offices they work in—because it can be so effective.
- “Malware” refers to various forms of harmful software, such as viruses and ransomware. Once malware is in your computer, it can wreak all sorts of havoc, from taking control of your machine, to monitoring your actions and keystrokes, to silently sending all sorts of confidential data from your computer or network to the attacker's home base.
- Attackers will use a variety of methods to get malware into your computer, but at some stage it often requires the user to take an action to install the malware. This can include clicking a link to download a file, or opening an attachment that may look harmless (like a Word document or PDF attachment), but actually has a malware installer hidden within.

PHISHING

- Of course, chances are you wouldn't just open a random attachment or click on a link in any email that comes your way—there has to be a compelling reason for you to take action. Attackers know this, too. When an attacker wants you to install malware or divulge sensitive information, they often turn to phishing tactics, or pretending to be someone or something else to get you to take an action you normally wouldn't. Since they rely on human curiosity and impulses, phishing attacks can be difficult to stop.
- In a phishing attack, an attacker may send you an email that appears to be from someone you trust, like your boss or a company you do business with. The email will seem legitimate, and it will have some urgency to it (e.g. fraudulent activity has been detected on your account). In the email, there will be an attachment to open or a link to click. Upon opening the malicious attachment, you'll thereby install malware in your computer. If you click the link, it may send you to a legitimate-looking website that asks for you to log in to access an important file—except the website is actually a trap used to capture your credentials when you try to log in.
- In order to combat phishing attempts, understanding the importance of verifying email senders and attachments/links is essential.

SQL INJECTION ATTACK

- SQL (pronounced “sequel”) stands for structured query language; it’s a programming language used to communicate with databases. Many of the servers that store critical data for websites and services use SQL to manage the data in their databases.
- A SQL injection attack specifically targets this kind of server, using malicious code to get the server to divulge information it normally wouldn’t. This is especially problematic if the server stores private customer information from the website, such as credit card numbers, usernames and passwords (credentials), or other personally identifiable information, which are tempting and lucrative targets for an attacker.
- An SQL injection attack works by exploiting any one of the known SQL vulnerabilities that allow the SQL server to run malicious code. For example, if a SQL server is vulnerable to an injection attack, it may be possible for an attacker to go to a website's search box and type in code that would force the site's SQL server to dump all of its stored usernames and passwords for the site.

CROSS-SITE SCRIPTING (XSS)

- In an SQL injection attack, an attacker goes after a vulnerable website to target its stored data, such as user credentials or sensitive financial data. But if the attacker would rather directly target a website's users, they may opt for a cross-site scripting attack. Similar to an SQL injection attack, this attack also involves injecting malicious code into a website, but in this case the website itself is not being attacked. Instead, the malicious code the attacker has injected only runs in the user's browser when they visit the attacked website, and it goes after the visitor directly, not the website.

- One of the most common ways an attacker can deploy a cross-site scripting attack is by injecting malicious code into a comment or a script that could automatically run. For example, they could embed a link to a malicious JavaScript in a comment on a blog.

- Cross-site scripting attacks can significantly damage a website’s reputation by placing the users' information at risk without any indication that anything malicious even occurred. Any sensitive information a user sends to the site—such as their credentials, credit card information, or other private data—can be hijacked via cross-site scripting without the website owners realizing there was even a problem in the first place.

DENIAL OF SERVICE (DOS)

- Imagine you're sitting in traffic on a one-lane country road, with cars backed up as far as the eye can see. Normally this road never sees more than a car or two, but a county fair and a major sporting event have ended around the same time, and this road is the only way for visitors to leave town. The road can't handle the massive amount of traffic, and as a result it gets so backed up that pretty much no one can leave.
- That's essentially what happens to a website during a denial of service (DoS) attack. If you flood a website with more traffic than it was built to handle, you'll overload the website's server and it'll be nigh-impossible for the website to serve up its content to visitors who are trying to access it.
- This can happen for innocuous reasons of course, say if a massive news story breaks and a newspaper's website gets overloaded with traffic from people trying to find out more. But often, this kind of traffic overload is malicious, as an attacker floods a website with an overwhelming amount of traffic to essentially shut it down for all users.
- In some instances, these DoS attacks are performed by many computers at the same time. This scenario of attack is known as a Distributed Denial of Service Attack (DDoS). This type of attack can be even more difficult to overcome due to the attacker appearing from many different IP addresses around the world simultaneously, making determining the source of the attack even more difficult for network administrators.

SESSION HIJACKING & MAN-IN-THE-MIDDLE ATTACKS

- When you're on the internet, your computer has a lot of small back-and-forth transactions with servers around the world letting them know who you are and requesting specific websites or services. In return, if everything goes as it should, the web servers should respond to your request by giving you the information you're accessing. This process, or session, happens whether you are simply browsing or when you are logging into a website with your username and password.
- The session between your computer and the remote web server is given a unique session ID, which should stay private between the two parties; however, an attacker can hijack the session by capturing the session ID and posing as the computer making a request, allowing them to log in as an unsuspecting user and gain access to unauthorized information on the web server. There are a number of methods an attacker can use to steal the session ID, such as a cross-site scripting attack used to hijack session IDs.
- An attacker can also opt to hijack the session to insert themselves between the requesting computer and the remote server, pretending to be the other party in the session. This allows them to intercept information in both directions and is commonly called a man-in-the-middle attack.

CREDENTIAL REUSE

- Users today have so many logins and passwords to remember that it's tempting to reuse credentials here or there to make life a little easier. Even though security best practices universally recommend that you have unique passwords for all your applications and websites, many people still reuse their passwords—a fact attackers rely on.
- Once attackers have a collection of usernames and passwords from a breached website or service (easily acquired on any number of black market websites on the internet), they know that if they use these same credentials on other websites there's a chance they'll be able to log in. No matter how tempting it may be to reuse credentials for your email, bank account, and your favorite sports forum, it's possible that one day the forum will get hacked, giving an attacker easy access to your email and bank account. When it comes to credentials, variety is essential. Password managers are available and can be helpful when it comes to managing the various credentials you use.
- This is just a selection of common attack types and techniques. It is not intended to be exhaustive, and attackers do evolve and develop new methods as needed; however, being aware of, and mitigating these types of attacks will significantly improve your security posture.

SOCIAL ENGINEERING

- Social engineering aims to convince a user to disclose secrets such as passwords, card numbers, etc. by, for example, impersonating a bank, a contractor, or a customer.

- A common scam involves fake CEO emails sent to accounting and finance departments. In early 2016, the FBI reported that the scam has cost US businesses more than $2bn in about two years.

- In May 2016, the Milwaukee Bucks NBA team was the victim of this type of cyber scam with a perpetrator impersonating the team's president Peter Feigin, resulting in the handover of all the team's employees' 2015 W-2 tax forms.

ABOUT US GLOBALY – AXIANS REDTOO

We are the Next Generation of passionately simple IT

In 25 years we have developed into one of the most successful IT consulting companies in Switzerland. We are strategic advisors and a full service provider with comprehensive know-how in one. Our customers benefit from a tailor-made combination of optimized business processes and efficiently implemented technology. We evaluate all processes and optimize your core business. We create the perfect system architecture and provide the best possible equipment. We ensure the smooth operation of all systems.

Founded in 1989
250 employees globally and growing
100% owner-operated & independent
43 Mio. US$ revenue (2015)

CH: Reinach, Basel, Bern, Zurich
AT: Vienna
CZ: Prague, Brno (Global SDC)
US: Florham Park (NJ), Fort Worth (TX)

ABOUT US GLOBALY – VINCI AND VINCI ENERGIES

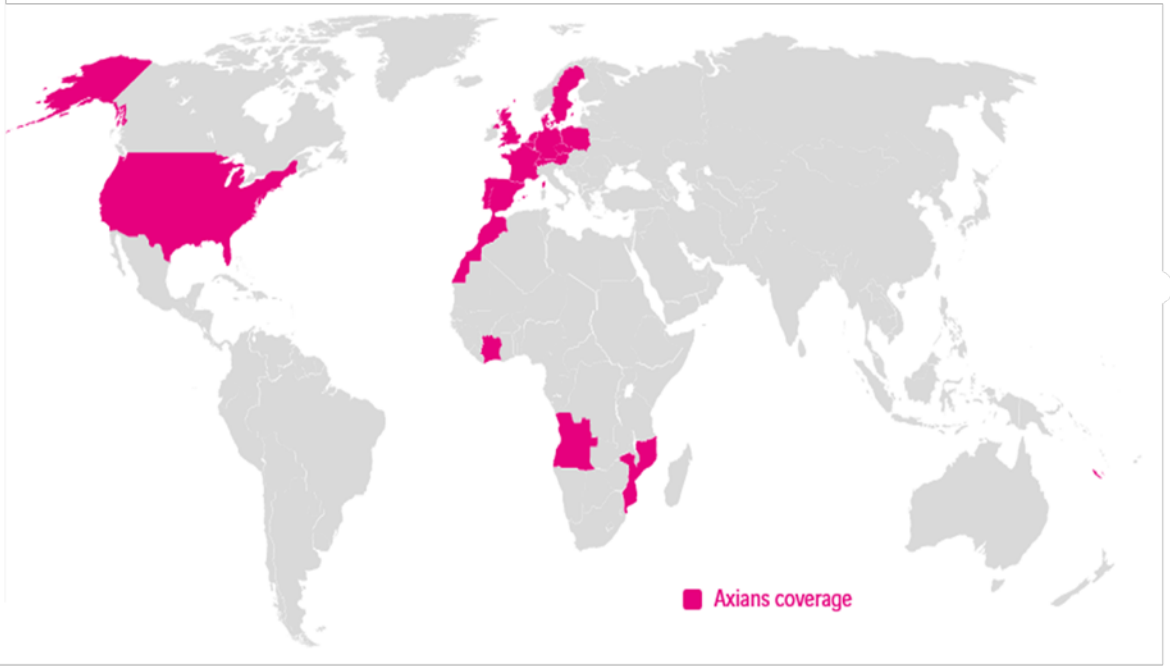
€ 1.8 bn
revenue in 2016

210
business units

8,000
employees

18
countries

- Angola
- Austria
- Belgium
- Czech Republic
- Denmark
- France / French overseas territories
- Germany
- Ivory Coast
- Morocco
- Mozambique
- Poland
- Portugal
- Spain
- Sweden
- Switzerland
- The Netherlands
- UK
- USA



AXIANS REDTOO – OUR SERVICES

Process Design

Design and optimization of business and IT processes, Workflow Development

Provision Services

Project Managers, **Developers**, Administrators, Network Specialists, Analysts, etc.

Projects

Application and infrastructure virtualizations, highly standardized **infrastructure** solutions, Infrastructure optimization

Managed Services

Building tailored & end-to-end services either on-site or off-site customer's location

Security

Information and data security, **IPS** (Intrusion Prevention Service), Penetration Tests, Security Audits

Internet of Things

Home automation system, Lighting control, Heating, A/C, Window blinds, Smart grid

Software Development Services

Development of custom solutions based on individual customer's needs together with our partner **uniCORE**

Science

Radiography, UV, Sonography, Monitoring of production parameters Active operations based on predictive models, scientific calculations