Is your service desk a security risk?

Social engineering attacks are ever more prevalent and yet the majority of support staff are completely unaware of the danger that 'doing a good job' might expose their employer to. Sensitive data and system login credentials may be accessed by unauthorised persons who use the simplest of techniques to lull the unwary service representative into willingly divulging commercially sensitive and confidential data. This article looks at how the security of your organisation may be breached by your support organisation's desire to provide a good level of service and how this risk can be mitigated.

Despite spending hundreds of millions of dollars each year on tools and services aimed at reducing exposure and risk; concerns regarding IT security regularly top the polls of IT leaders concerns. There is an innate belief that the other guy is always out to get us and that IT has in some way made it easier for them to do just that. This paranoia is compounded by the news which is filled with stories of cyber crime, identity theft and e-fraud. Consequently, every organisation has been convinced that they need to put in place measures to counter this perceived threat. Unfortunately many of the security toolsets out there are focused upon risks which are relatively rare and in reality may never endanger the majority of businesses. And yet the risks are real. Not the risks from faceless cyber terrorists on the other side of the world attempting to penetrate your corporate network using state of the art hacking techniques. No. But, the real risks come from a much less high tech source. The majority of the security tools on the market forget the human factor. And it is the human factor that the most successful e-criminals use to best effect.

Social engineering is the current name for one of the oldest criminal talents – the skill of the con artist. By convincing someone to willingly do something that they wouldn't do at all if they had a full understanding of the circumstances and the consequences of their actions the perpetrator can penetrate even the most secure of systems or environments.

The tools of the social engineers trade include:

- Research – Knowing the target's business and internal processes better than they know them themselves
- Impersonation – Assuming the identity of a legitimate customer or user (usually someone of seniority or with an association with a senior executive)
- Establishing plausibility – Name dropping, Mentioning internal events / announcements, Awareness of corporate procedures and systems etc
- Ingratiating themselves – Overly friendly manner, Gushing thanks and praise for minimal help
- Misdirection – Asking on behalf of someone else, Asking for more than required and accepting less, Requesting seemingly innocuous information which they can then use to their advantage
- Peer pressure – Suggesting that others with the organisation have already assisted them e.g. Such and such just gave me their data, can you give me yours too?
- Confidence and demeanour – Sheer weight of personality, tone of voice and intonations in the pattern of speech all come together to help make the target completely believe what they are being told
- Timing – With fraud as with comedy, timing is everything. The expert social engineer will carefully plan their interactions to coincide with shift changes, times with low staff levels (e.g. out of hours, lunch times, statutory holidays etc), busy periods etc.
- Targeting – Advanced attackers will study their potential targets carefully before making a move and will often pick off the weakest in the group (e.g. a new starter) deliberately to increase their likeliness of success.

Given the powerful array of tools available to the social engineer is it any wonder that many seemingly savvy individuals fall prey to their advances? So how can you prevent your

service desk falling foul of such attacks? The following list outlines some of the key actions that every service desk should undergo to mitigate the risk of succumbing to a social engineering attack.

- Review and revise security policy if required – Everything should flow from the security policy. The policy should clearly explain what is acceptable and what isn't. This can help deflect animosity and aggression towards the support desk when they unavoidably slow down the call process in order to verify the caller's identification etc.
- Education / Training for all support personnel – The most critical element of the countermeasures against social engineering attacks are the people who will be attacked themselves – They are the first and last line of defence!
- Awareness programmes – Even memories of the best training courses fade. In order to maintain the focus it is necessary to repeat education and messaging from time to time.
- Define the entitlement process – Many service desks do not have formal entitlement checks in place. This omission must be corrected. The processes needn't be overly complex (E.g. requiring a retinal scan, blood sample and a signed letter from the requesters great-grandparents may be a little extreme for instance) but they must be adequate and applied consistently.
    - Definitions of entitlement – Entitlement used to be limited to identifying who was supposed to have access to receive service and support. Nowadays, it is also critical to ensure that there is also a definition of what it is they have access to as well in order to act as a second line of defence against an attacker that has successfully managed to breach the outer perimeter as it were by successfully impersonating an individual that has access.
    - Identification validation process – The process needs to be self maintaining and stream lined enough to prevent excessive delays. A system where the user is required to provide the x and y characters of a regularly changed password is usually sufficient.
- Implement a service catalogue – Identification validation checks without the appropriate integrations to a service catalogue can only ever validate one piece of the complete entitlement picture. If a person's true entitlement is to be understood the service desk solution must be seamlessly integrated with a service catalogue that clearly defines the nature and scope of the services to be provided to the individual and the necessary approval cycles that must be run for potentially sensitive requests.
- Tighten integrations with other systems e.g. HR tools
    - Vacation details – By tying the vacation tracking system into the service desk solution agents can be alerted about requesters that are calling when they are scheduled to be on vacation – whilst not a definitive test, it is likely that social engineering attackers may try to assume the identity of persons that are absent to minimise the likelihood of discovery.
    - Training history – Details of the requesters training history may be used as an additional validation point during the identity validation process e.g. Which training course did you take in February? Where was it held? etc

The above list of control measures clearly demonstrates the importance of staff training. But what exactly are they supposed to learn? Thankfully, many people working in the support arena are already blessed with a healthy dose of cynicism. All that is often required is the identification of potential risk scenarios and some guidance on what to do with a suspicious caller or email. However for the more trusting folks it is as well to highlight the following points so that there is no confusion over the risks and possible signs that all is not as it should be.

Is your service desk a security risk?

- Communication channel trustworthiness – How has the request reached you?
  - Telephone calls – Can you be certain the call is from where you think it is?
    - Internal transfers
    - Masked / withheld numbers
    - Public extension within the premises
  - Email – Is there any reason to suspect the validity of the email?
    - Non-work email accounts
    - Phishing / Spoofing
- Anomalies – Is there anything whatsoever that is causing suspicion or concern?
  - Time of request / Unusual call patterns e.g. increased frequency
  - Mistakes with details / Inconsistencies in their story
  - Call back number different to the user's normal office or mobile number
- Request context – Does the request sit right in the current climate?
  - Is a salesperson requesting access to a non-sales system etc
- Pretext validation for the request – Does their story add up?
  - Is the reason for the request given by the caller plausible?
- Entitlement checking – Are they entitled to receive what they have asked for?
- Delivery security – Do they want the service delivered using normal channels?
  - Asking for account credentials over the phone
  - Sending information to non-corporate email addresses
  - Requesting to pick equipment up in person or having it delivered to a non-work location
- Identity verification – Who is the requester claiming to be? Can they prove they are who they say they are?
- Evasive manoeuvres – Is the caller hesitant to provide information about themselves?
  - Did they offer to call back rather than be called?
- Manner – Are they anxious, over confident, aggressive?
  - Are they more aware than the average user as to what they want or need?

Hopefully this article hasn't caused you too much discomfort, or created an ominous sense of unease. Whilst the risks are real and serious; the control measures required to mitigate them are within the reach of every organisation. The price of security is eternal vigilance but this doesn't mean that it should become an all consuming obsession. By taking a proactive stance and educating your team to the potential dangers you will be ahead of the game and should help avoid a costly and/or embarrassing social engineering based security breach. To quote Nick Ross from the BBC's Crime Watch, "Don't have nightmares!"

Rob Addy is the author of "Effective IT Service Management: To ITIL and beyond!". Full details may be found at:

www.effectiveitsm.com
www.springer.com/978-3-540-73197-9