SOCIAL ENGINEERING IN DE INFORMATIEBEVEILIGING

Andres Rutkens, Adviseur social engineering – Stichting CHORUS

Cybercriminele aanvallen zijn niet alleen op technologie, maar steeds meer op de mens gericht. Het zijn immers de gebruikers van Informatie Technologische middelen die toegang hebben, of kunnen verlenen tot de waardevolle informatie. Ten opzichte van de technische kennis en de investeringen op technisch vlak in de informatiebeveiliging is de menselijke factor onderbelicht. Daardoor is de mens de zwakste schakel. Hierdoor vormt Social Engineering een steeds relevantere bedreiging voor IT-security. Gebruikers worden misleid door cybercriminelen die op die manier informatie kunnen verkrijgen. Hoe gaan Social Engineers daarbij te werk en hoe kunt u ze stoppen?

Social Engineering zien we voornamelijk terug in twee stromingen: Social Engineering gericht op grote groepen in de maatschappij en gerichte Social Engineering om maatregelen in de informatiebeveiliging te omzeilen.

De eerste variant heeft vaak tot doel de samenleving te fragmenteren of zelfs te destabiliseren ten behoeve van invloed en macht. De gerichte beïnvloeding door Cambridge Analytica[1] in Afrika en het westen, Chinese gamification of control[2] en Russische Troll-farms[3] zijn recente voorbeelden. Bij de tweede variant heeft Social Engineering het doel om toegang te faciliteren en waardevolle informatie te verkrijgen, de CEO-fraude, de Bangladesh-hack en de Democratic National Committee(DNC) -hack zijn daar voorbeelden van. De combinatie van DNC- hack, Cambridge Analyitica en Troll-farms bleken elkaar te versterken tijdens de verkiezingen in de Verenigde Staten, de gevolgen zien we dagelijks terug in het nieuws. We kunnen de verschillende stromingen dus niet meer los van elkaar zien.

Deze whitepaper is gericht op de gatekeepers van informatie. De informatiebeveiligers. Daarom focususen we in deze whitepaper op Social Engineering die we tegenkomen in de informatiebeveiliging.

WAT IS SOCIAL ENGINEERING?

De definities van maatschappelijke Social Engineering en de variant gericht op informatiebeveiliging verschillen. De basis van gedragsbeïnvloeding zien we wel terug in beide stromingen.

Maatschappelijk

"The use of centralized planning in an attempt to manage social change and regulate the future development and behaviour of a society."

Informatiebeveiliging

"The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes."[4]

De verschillen

De voornaamste verschillen zijn het doel en de slachtoffers. Maatschappelijke Social Engineering ontwricht samenlevingen en manipuleert grote groepen burgers. Social Engineers werken dan ook vaak in opdracht van statelijke actoren. De Social Engineers die we in de informatiebeveiliging tegenkomen zijn vooral uit op zeer waardevolle informatie, kroonjuwelen waar ze veel geld voor kunnen krijgen. Hiervoor richten zij hun peilen op specifieke mensen in uw organisatie.

De overeenkomsten

Zijn er dan ook overeenkomsten? Jazeker. Bij beide vormen van Social Engineering draait het om vergaren van informatie, deze informatie misbruiken en toegang daartoe verkrijgen. De informatie is essentieel. Social Engineers zijn uit op user data, zoals nationale geheimen over bijvoorbeeld atoomprogramma's, buitenlands beleid en economische informatie. Kortom: Waardevolle informatie – al verschillen de doelstellingen waarvoor ze deze informatie proberen te achterhalen. Social Engineers misbruiken altijd de menselijke factor om toegang te krijgen tot deze waardevolle informatie. In de meeste gevallen bevindt deze informatie zich in beveiligde systemen, met Informatiebeveiliging-professionals als de gatekeepers. De informatiebeveiligers en hun maatregelen omzeilen is dus een belangrijk doel. Vooralsnog zijn de maatregelen vooral IT gericht. Dit is een voordeel voor de Social Engineer, want IT'ers zijn vaak gericht op techniek en minder op de menselijke factor. De gebruikers van de IT-systemen zijn daarmee een ideaal doelwit.

Beide vormen van Social Engineering zijn met elkaar verweven. Bij economische spionage en sabotage overlappen handelingen van 'cybercriminele' Social Engineers het meest

met ‘statelijke gesteunde’ Social Engineers. Hierbij gebruiken Social Engineers digitale middelen zoals bijvoorbeeld botnets en phishing mails; phishing mails om gevoelige informatie of toegang te verkrijgen en Botnets om op social media de publieke opinie te beïnvloeden. Botnets worden ook gebruikt voor DDOS. Dat laatste kun je misschien geen echt hacken noemen, maar het frustreert wel systemen en websites.

Een algemeen en sprekend voorbeeld van Social Engineering is CEO-Fraude. Hierbij doen Social Engineers alsof ze de CEO of CFO zijn. Vaak ontvangt een financiële medewerker hierbij een e-mail van de baas die hem opdraagt met spoed een fors bedrag over te maken naar een ‘zakenpartner’. Ter verificatie kan hij het advocatenkantoor bellen, dat in het complot zit. Bij de grootste bank-hack ooit, de eerder genoemde Bangladesh bank-hack, werd deze methode groots ingezet. Complete transactieprocessen werden nagebootst (*spoofing*). Dat leverde de aanvallers meer dan 850 miljoen US dollar op. Deze aanvallen gaan niet over ‘één nacht ijs’ en zijn goed voorbereid.

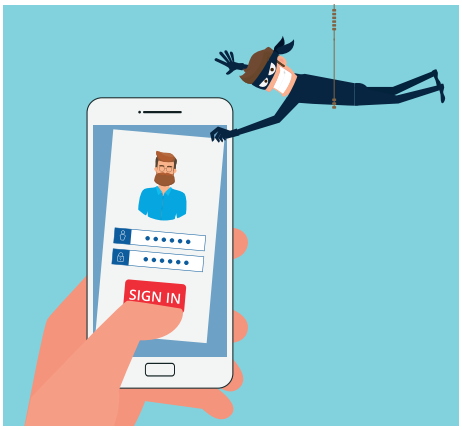
DE OPKOMST VAN SOCIAL ENGINEERING

Social Engineering is hot. Niet alleen de kwantiteit, ook de kwaliteit neemt toe. Daarvoor zijn drie hoofdredenen.

In de huidige informatiesamenleving is data het nieuwe goud. Deze informatie is geld waard, denk aan creditcardgegevens, BSN-nummers, patiëntendossiers en gebruikersdata. Vooral deze laatste categorie wordt steeds belangrijker. Daarnaast is bedrijfkritische informatie over bijvoorbeeld productieprocessen, klantenbestanden en aanbestedingstrajecten veel geld waard.

Een tweede reden voor de toename van Social Engineering is de voortschrijdende security-technologie. Inderdaad, dat maakt de mens steeds vaker de zwakste schakel. Maar hier zit meer achter. Verouderde technologie en de menselijk factor behoren beiden immers al langer tot de twee kwetsbare aspecten van informatiebeveiliging. De afgelopen decennia hebben we ons gefocust op het verbeteren van de technologie en boeken we hierin vooruitgang. Daarbij is de menselijke factor vaak onderbelicht gebleven. Misschien omdat de technologie continu verandert en de mens niet? Een soort ‘voldongen feit – gedachte’.

Technologie ontwikkelt snel, de mens langzaam. Bij Social Engineering maakt men gebruik van ‘klassieke’ toepasbare beïnvloedingsmethoden in combinatie met steeds vernieuwende technische middelen. Dat maakt ons nog kwetsbaarder[5]. Dat is een derde verklaring voor de opkomst van Social Engineering. Ons brein is over een periode van tienduizenden jaren geëvolueerd. Daarbij zijn shortcuts in onze denkwijze ontstaan. Manieren die ons helpen om snel te kunnen inschatten of iets wel of niet veilig is[6]. Bij het oversteken van de straat letten we bijvoorbeeld op het groene stoplicht, zebrapad en tegemoetkomende voetgangers. Niet op het nummerbord van een passerende auto of fotograferende dame op de hoek. Door deze shortcuts in ons denken, kunnen we ook snel prioriteiten stellen bij een overvloed aan informatie, maar missen we misschien de informatie waar het echt om gaat. Denk aan een link die niet klopt in een phishing mail met een op het oog betrouwbare afzender.



Of we vertrouwen een gesprekspartners op basis van herkenbaarheid of de autoriteit die hij uitstraalt. Werkt die aardige man op het congres net als jij ook op de ICT-afdeling van een verzekeraar, dan zul je daar makkelijker vakinhoudelijke info mee uitwisselen dan wanneer deze man in een totaal andere omgeving zou werken dan jij.

HOE GAAN SOCIAL ENGINEERS TE WERK?

Social Engineers nemen de tijd. Ze bereiden zich voor en targeten verschillende personen op uiteenlopende manieren – fysiek en digitaal. Zo vinden ze alle puzzelstukjes aan informatie. Deze combineren ze om uiteindelijk het totaalplaatje helder te krijgen om toegang tot de gewenste bedrijfsinformatie te kunnen krijgen. Wat zijn de verschillende zwakke plekken die ze uitbuiten, met welke methoden en hoe herkent u die?

Heuristieken

Social Engineers misbruiken universele menselijke denkstrategieën, de eerder benoemde shortcuts in onze denkwijze, die we als mens ontwikkeld hebben in een periode ver voor het digitale tijdperk. Deze strategieën voldoen niet meer voor onze huidige tijd, maar toch passen we ze nog onbewust toe waardoor ze denkfouten veroorzaken in ons brein. Deze fouten zijn vaak lastig te herkennen. Een paar belangrijke voorbeelden (er zijn meer):

1 Representatie

Iemand heeft bijvoorbeeld de uiterlijke kenmerken van een bepaalde groep. Daardoor nemen we snel aan dat hij ook de innerlijke kenmerken heeft. Wanneer we iemand met een witte jas en stethoscoop zien, denken wij al snel dat het een arts is. Iets wat herkenbaar is, accepteert men sneller en ziet men dan eerder aan voor waar en betrouwbaar.

2 Beschikbaarheid

We nemen de beschikbare informatie snel als waarheid aan. Denk bijvoorbeeld aan de algoritmes die informatie op social media beschikbaar maakt. Ook wat we op TV zien, vinden we meestal relevant. Wanneer de NOS het nieuws brengt, gaan we er vanuit dat dit waar is. Maar weten we dat wel zeker?

3 Framing

De context is bepalend. Doordat iets plaatsvindt in een herkenbare omgeving, concludeert ons brein automatisch dat het waar is. Iemand in een lange witte jas zien we als arts als hij in het ziekenhuis rondloopt, maar niet wanneer we deze persoon de kroeg tijdens carnaval tegenkomen.

4 Quid Pro Quo

Voor wat, hoort wat. U vertelt mij wat, ik vertel u wat. Mensen zijn geneigd sneller informatie te delen wanneer hun gesprekspartner dat ook doet.

5 Commitment en consistentie

Wie A zegt moet ook B zeggen. We zijn gewoontedieren en we zijn principieel, waardoor we soms de voordehand liggende keuze maken in plaats van de juiste. Resultaten uit het verleden zijn geen garantie voor de toekomst.

Gedragskenmerken

Naast heuristieken hebben we universele gedragskenmerken. Door die te kennen en daar slim gebruik van te maken, kunnen Social Engineers slachtoffers manipuleren. Een paar voorbeelden van kwetsbare universele gedragskenmerken:

- Behoefte aan erkenning, zoals een compliment over vakkennis.
- Neiging om commentaar te hebben op en te roddelen over een derde (zoals een werkgever).
- Gebrek aan een luisterend oor, mensen praten graag en willen graag gehoord worden.
- Neiging om jezelf bescheiden op te stellen: 'ik had het niet gekund zonder mijn collega's'.
- De onbewuste wil om geheimen te delen.
- Rol student-docent: de student luistert waardoor de docent (zijn mond voorbij) praat.
- Onderschatten van de informatiewaarde. Losse informatie is waardevol in combinatie met andere puzzelstukjes.[7]

DE METHODEN VAN SOCIAL ENGINEERS

Bij het misbruik maken van menselijke heuristieken en gedragskenmerken, hanteren Social Engineers verschillende methoden. De drie belangrijkste zijn profiling, pretexting, rapport building en ontlokking.

Profiling

Voordat Social Engineers hun daadwerkelijke zoektocht naar informatie beginnen, brengen ze een organisatie, de teams en werknemers in kaart. Profiling wordt dat genoemd. Daarbij geldt: kennis is de sleutel tot succes. Social Engineers willen onder andere weten hoe een organisatie en haar processen in elkaar steken, wie verantwoordelijk en geautoriseerd is om bepaalde processen te stoppen of te starten, hoe dat gebeurt, wie er op welk moment kwetsbaar is en wat voor persoonlijkheid iemand heeft.

Op basis van profiling kunnen Social Engineers heel gericht verschillende personen targeten om vervolgens te manipuleren en de gewenste puzzelstukjes te bemachtigen. Deze informatie combineren ze met gedetailleerde informatie over de persoon. Zo kunnen ze in een later contact bijvoorbeeld beter aan rapport building doen: wanneer ze iemands karakter kennen, weten ze zijn gedragskenmerken. Tijdens profiling leggen Social Engineers de sterke en zwakke punten van potentiële targets vast. Daardoor kunnen bijvoorbeeld voorspellen hoe iemand in een conflictsituatie handelt en hun plan daarop afstemmen.

Pretexting

Pretexten zijn de valse voorwendselen die de Social Engineer creëert en gebruikt om zijn acties af te stemmen op de situatie en zijn eigen handelingen af te schermen. De pretext is zo opgezet dat het perfect past bij de te behalen doelen (toegang, of ontlokken van informatie) en het geeft de Social Engineer de perfecte frame om zijn doelwit te manipuleren. Om dat zo goed mogelijk te kunnen doen, analyseren ze al in een vroeg stadium de gedragsstijlen van hun slachtoffers, profiling. De grond is vruchtbaar gemaakt voor rapport building.

Rapport building

Social Engineers zoeken aansluiting bij hun slachtoffer door wederzijds vertrouwen en begrip te creëren. Dat begint met het vergaren van persoonlijke kennis. Hoe zit iemand in elkaar: heeft hij een dominant, terughoudend, ondersteunend of harmonieus karakter? Daar maken ze gebruik van in verbale en non-verbale communicatie. Bijvoorbeeld door gedrag te spiegelen of juist niet. Een dominante persoonlijkheid kan bijvoorbeeld eerder informatie loslaten als de gesprekspartner zich juist onderdanig opstelt. Elke persoonlijkheid is geneigd om in een bepaalde situatie anders te reageren. Er zijn diverse methoden om te achterhalen hoe iemands karakter in elkaar zit. Via boeken en cursussen kan elke Social Engineer zijn rapport building-skills verder ontwikkelen.

Ontlokking

Deze methode wordt ook wel 'elicitation', of ontlokking, genoemd en is zowel gericht op het verkrijgen van de gewenste informatie in een gesprek als op het maskeren van de daadwerkelijke informatiebehoefte. Social Engineers vragen niet rechtstreeks naar een wachtwoord, mislukte update of inlogprocedure. Door het uitlokken van, en inspelen op gedrag, krijgen ze toch de gewenste antwoorden — zonder dat de gesprekspartner zich er van bewust is dat hij of zij waardevolle informatie prijsgeeft. De gestelde vragen sturen het gesprek en maskeren het doel van de Social Engineer.

Bij ontlokking maken Social Engineers misbruik van heuristieken en gedragskenmerken. Nog steeds gebeurt dit gewoon in het gesprek. Bijvoorbeeld door breed, met open vragen te beginnen en daarna het gesprek met gesloten vragen te sturen naar het gewenste onderwerp. Wanneer ze te weten zijn gekomen wat ze willen, maskeren ze dit door het gesprek weer een andere kant op te sturen met open vragen. Deze sturende en tegelijkertijd maskerende gesprekstechniek — van macro, naar micro en weer naar macro — wordt ook wel het zandlopermodel genoemd[8]. Door aantrekkelijke en toepasselijke framing is er ruimte voor manipulatie van gedragskenmerken. Zo vormt de Social Engineer het gedrag naar een gewenste handelingen. Dit gebeurt ook in digitale vorm. Toegang en informatie verkrijgen is nog steeds het doel.

De werkwijze bij ontlokking is niet in beton gegoten. Social Engineers stemmen hun technieken af op de hoeveelheid tijd die ze hebben, de dynamiek, (digitale) omgeving en de setting. In de huidige digitale wereld zien we de methoden van ontlokking terug in vele verschillende en steeds veranderende digitale tactieken.

PRAKTIJKVOORBEELDEN VAN SOCIAL ENGINEERING

In de praktijk maken Social Engineers gebruik van verschillende methoden. Grote kans dat ze in één poging profiling, pretexting, rapport building en ontlokking combineren. Hieronder enkele voorbeelden van de Social Engineer Kevin Mitnick[9]. Hij beschrijft trucjes die veel worden toegepast. Maar wat zijn de achterliggende methoden om deze trucjes te laten werken? De trucjes hebben we daarom aangevuld met achtergrondkennis.

Gevonden USB-stick

Een medewerker vindt een USB-stick. 'Van wie zou die zijn? Als ik die inplug zie ik dat vanzelf'. Ondertussen besmet hij het netwerk met malware. Hij is in een bekende omgeving, vertrouwt deze omgeving inclusief de attributen die er aanwezig zijn, zoals een USB-stick. Inmiddels is deze methode steeds meer achterhaald, omdat organisaties deze effectief tegengaan door USB-poorten op slot te zetten.

Phishing mail

Goede phishing mails zijn overtuigend: ze lijken via een bekend en vertrouwde instantie, zoals een bank of verzekeraar te komen. De beschikbare informatie (pretext) staat in een goed geframede e-mail, bevatten een informatieoverload, sense of urgency (behoefte om het goed te willen doen, erkenning) en een link. De verleiding om te klikken is dan groot.

Spearphishing

Met een geaccepteerd vriendschapsverzoek voor social media kan de Social Engineer achter persoonlijke info van vrienden komen. Ook via gesprekken is goed te achterhalen hoe mensen onderling communiceren op het werk. Om zich vervolgens in een spearphishing mail voor te doen

als een vriend of collega. Beschikbaarheid van informatie is bijvoorbeeld: ik ben je vriend. Daardoor is de representativiteit perfect om de ander te laten klikken. Dit vooral omdat de 'relatie' een bepaalde commitment en consistentie kent.

Voice phising
Een Social Engineer doet zich voor als medewerker van de helpdesk, bank of verzekeraar. Hij overtuigt de beller met gedetailleerde voorkennis. Door de persoon aan de andere kant van de lijn te profilen, een goede pretext en rapport building toe te passen gaat dit gemakkelijker dan je denkt.

Fysieke kantoorbeveiliging
Social Engineers glippen soms met medewerkers mee naar binnen na hun rookpauze of in de ochtenddrukte. Dit werkt goed bij grote organisaties waar niet iedereen elkaar kent. De Social Engineer gebruikt hierbij zijn voorbereiding en voorkennis van de organisatie en personen in de organisatie. Hij weet van te voren wat hem verder brengt. Nog beter zou het zijn als hij iemand anders die al binnen werkt, een medewerker, zover kan krijgen dat hij van deze medewerker informatie kan ontlokken. Misschien is een 'perfecte' kennismaking met de medewerker tijdens een congres een begin?

Vriendelijke support medewerker
Problemen met software of hardware? Dat heeft de zogenaamde helpdeskmedewerker of leverancier zo voor u opgelost. 'Wat is uw wachtwoord? Dan kan ik meekijken op uw computer'. De medewerker gaat er vanuit dat de support ook daadwerkelijk support is. Er wordt informatie beschikbaar en geframed. Een vriendelijk persoon (rapport building) helpt je verder (Quit pro quo, behoefte aan erkenning). Waarom zou u die niet willen vertrouwen?

De reiziger
Daarnaast zijn er nog een aantal voorbeelden. Vooral in bedrijfsspionage wordt gevoelige informatie ontlokt vanuit reizende medewerkers. In hotels, vluchthavens en ander locaties, denk bijvoorbeeld aan conferentielocaties. In een hotelkamer verblijven we meestal relatief kort. Soms een paar dagen, soms een week. Maar we beschouwen de hotelkamer en lounge al snel als ons thuis, weg van huis. En onze mede-professionals als vrienden waarmee we na een lange dag een biertje gaan drinken. En dan moeten we toch echt even 'stoom afblazen'.

De insider
De complexe en langdurige benaderingen gaan verder dan het vorige voorbeeld. In sommige gevallen gaat het veel verder dan een trucje op korter termijn. Een investering die vaak heel veel oplevert voor de Social Engineer, veel meer dan in de vorige voorbeelden. Het gehele proces van profiling, pretexting, rapport building en ontlokking is dan een doorlopend proces. Men komt steeds dichterbij de juiste mensen en geheime informatie. De 'juiste' mensen worden benaderd. Zij kunnen toegang tot de juiste informatie verlenen. Het kan zo ver gaan dat het (voormalige)doelwit volledige medewerking gaat geven en zelfs eigen manieren gaat ontwikkelen met de Social Engineer om geheime informatie te ontlokken en over te dragen.

WAT KUNT U DOEN TEGEN SOCIAL ENGINEERING?

Social Engineers op serieus niveau zijn tegenwoordig goed voorbereid. Zij besteden aandacht aan details en denken niet in grenzen maar mogelijkheden. Daarom is de pentesting, het testen van de toegang en van beveiliging systemen, niet altijd effectief. Vooral omdat de grenzen van het te testen gebied al vastgelegd is. Deze grenzen worden juist overschreden door de Social Engineer. Zelfs red teaming, het testen van de informatiebeveiliging zonder de testers en het aanvalsoppervlakte teveel in te kaderen binnen grenzen, is niet altijd effectief genoeg. Dat komt vooral omdat de testen op technisch vlak ver zijn ontwikkeld, in tegenstelling tot de menselijke factor. En men is er nog niet helemaal uit hoe de aanval via de menselijke factor te doen zonder ethische grenzen te overschrijden en commercieel aantrekkelijk uit te voeren. Kennis en kunde op het gebied van Social Engineering ontbreekt simpelweg.

Wanneer u weet hoe Social Engineers werken, kunt u hun methoden herkennen. Dus kennis van hun werkwijze, is essentieel. Hebt u een Social Engineer door? Dan kunt u hem tegenhouden en zelfs zijn eigen methoden op de aanvaller loslaten om erachter te komen naar welke info hij op zoek is of wie zijn opdrachtgever is.

U kunt uzelf en uw organisatie op drie manieren eenvoudig weerbaarder maken tegen Social Engineering:

> Knowledge is power. Information is liberating. Education is the premise of progress, in every society, in every family
>
> – Kofi Annan

1 Weet hoe Social Engineers werken – wanneer u hun methoden en manipulatietechnieken kent, kunt u die herkennen en eventueel de rollen omdraaien.
2 Wees bewust van uw menselijke denkstrategie – de shortcuts in uw brein kunt u niet uitzetten, maar wees alert dat u ze maakt. Vooral wanneer er gevoelige onderwerpen aan bod kunnen komen of er stressvolle situaties ontstaan.
3 Ken uw eigen risicoprofiel – weet welke informatie gevoelig is, en wie er toegang toe heeft.. De conciërge of systeembeheerder vindt zichzelf misschien onbelangrijk binnen een organisatie, maar kan voor Social Engineers wel een essentiële pion zijn.

Een open houding betekent niet dat u naïef moet zijn. Plaats voor uzelf piketpaaltjes: bepaal over welke onderwerpen u niets vertelt aan vreemden. Komt iemand in de buurt van deze kroonjuwelen, dan gaan de alarmbellen vanzelf af. Zorg dat u kennis van zaken heeft op het gebied van Social Engineering. Bespreek de bescherming van uw kroonjuwelen intern en deel uw Social Engineering kennis ook met collega's, zodat uw hele team weerbaarder wordt. Uw security is immers maar zo sterk als de zwakste schakel.

Hoe nu verder?
Bij elke organisatie in elke sector zijn Informatiebeveiligers en IT-professionals de gatekeepers. Zij bewaken de informatie waar een Social Engineer op uit is. Voor organisaties die hun security willen wapenen tegen Social Engineering, zijn er diverse cursussen.

[1] https://www.nytimes.com/2017/03/06/us/politics/cambridge-analytica.html
[2] https://media.ccc.de/v/34c3-8874-gamified_control
[3] http://www.bbc.com/news/technology-43093390
[4] Oxford Dictionary, https://en.oxforddictionaries.com/definition/social_engineering
[5] *The internet of us*, Michael Patrick Lynch
[6] Robert Cialdini, influence
[7] *Business secrets. Getting theirs – keeping yours*, John Nolan
[8] *Business secrets. Getting theirs – keeping yours*, John Nolan
[9] *The Art of Intrusion*, Kevin D. Mitnick William L. Simon