Experts in Training & Conferences
an informa business

whitepaper

7 verborgen manieren waarop menselijk gedrag uw beveiliging ondergraaft

WEBWERELD CUSTOM

7 verborgen manieren waarop menselijk gedrag uw beveiliging ondergraaft

Ondanks alle technologische maatregelen die getroffen worden, blijven bedrijven kwetsbaar voor cybercriminaliteit. Want hoe goed de beveiliging ook is, de zwakste schakel is en blijft de mens. Op welke manieren ondermijnt menselijk gedrag de beveiliging van uw bedrijf?

Wachtwoorden

Medewerkers gebruiken het liefst makkelijk te onthouden wachtwoorden. Helaas zijn die bijzonder eenvoudig en snel door een kwaadwillende te achterhalen via bijvoorbeeld een brute force aanval. Ook zijn de beveiligingsvragen die als geheugensteuntje dienen, vaak ideaal om het wachtwoord zelfs helemaal te omzeilen. Een zoektochtje op internet of social media is meestal voldoende om vragen als “in welke stad ben je geboren” en “hoe heet je huisdier” te beantwoorden.

Om het nog erger te maken, geeft één account vaak toegang tot een hele keten aan systemen, of hetzelfde wachtwoord wordt voor meerdere websites en informatiesystemen gebruikt. Het is voor aanvallers dan ook zeer lucratief om een gebruikersaccount te kraken. Het risico wordt nog eens vergroot doordat gebruikers hun wachtwoorden meestal pas veranderen zodra het systeem erom vraagt en ze echt niet anders kunnen. Heeft een hacker eenmaal toegang, kan er dus lang misbruik gemaakt worden.

hetzelfde wachtwoord wordt voor meerdere websites en informatiesystemen gebruikt.

Een organisatie kan dit allereerst afvangen door bewustzijn bij medewerkers te kweken. Maak duidelijk wat de risico’s zijn en hoeveel schade het oplevert.

Daarnaast blijft een goed wachtwoordbeleid nodig. Bepaal de eisen die aan wachtwoorden worden gesteld en laat het systeem dit afdwingen. Denk aan de complexiteit van wachtwoorden en de houdbaarheid.

Phishing en malware

We openen nagenoeg alle e-mails die binnenkomen en vaak klikken we op links zonder voldoende stil te staan bij de risico’s. Maar berichten zijn niet altijd van de personen of bedrijven waar ze van afkomstig lijken. Gelukkig vallen veel nepberichten direct door de mand door slecht taalgebruik en inconsistenties in de tekst, maar dan nog blijven er genoeg gevaren over. Vooral als een bericht er betrouwbaar uitziet of van bekenden afkomstig lijkt, openen we een bijgesloten bestand of link zonder er al te veel bij na te denken. Zo besmetten we onbedoeld systemen, met alle gevolgen van dien.

Malware kan soms jarenlang stukjes informatie verzamelen en doorsturen zonder dat iemand het merkt. Het is dan ook van belang om een goede filtering te hebben, zodat valse berichten al op de mailserver worden onderschept. Daarnaast is het belangrijk bewustzijn te kweken dat medewerkers berichten goed moeten lezen en de daadwerkelijke afzender moeten controleren. Ook is het nodig links in berichten te analyseren om te zien naar welke websites ze echt doorverwijzen. Bijlagen mogen nooit

zomaar worden geopend. Een bekende truc is de factuur die geen pdf maar een uitvoerbaar bestand blijkt te zijn. Tot slot is het cruciaal dat medewerkers een eenmaal ontdekte bedreiging direct melden, zodat de filtering kan worden bijgewerkt en de organisatie kan worden ingelicht.

Bring Your Own Device (BYOD)

We werken al lang niet meer met alleen maar bedrijfsapparatuur en ook niet meer alleen op kantoor. Dat maakt het lastiger om apparatuur centraal te beveiligen en te beheren. Werknemers nemen bijvoorbeeld een laptop mee naar huis, of werken op openbare plekken zoals het station of een terras. Daarnaast gebruiken we steeds vaker onze eigen spullen, denk aan laptops, tablets en smartphones. Een privé-laptop is gelukkig vaak wel beveiligd met een virusscanner, maar toch gaan werknemers er meestal wat makkelijker mee om. Want het staat toch los van de zaak, dus welke schade kan het aanrichten? Terwijl een thuis of onderweg besmette laptop eenvoudig het bedrijfsnetwerk van binnenuit kan infecteren.

Al deze apparatuur moet dan ook extra goed beveiligd worden. Met een up-to-date virusscanner, een actieve firewall en updates die automatisch worden opgehaald en geïnstalleerd. Vooral als er niet alleen vanaf afstand wordt gewerkt, maar apparatuur ook op het interne netwerk wordt aangesloten. De IT-afdeling kan hierbij helpen. Met advisering en het beschikbaar stellen, installeren, configureren en up-to-date houden van de benodigde tools.

“Bring Your Own Tools”

De IT-afdeling stelt doorgaans alle benodigde apparatuur en software beschikbaar. Alleen weten gebruikers tegenwoordig heel goed zelf wat er allemaal beschikbaar is aan handige en slimme tools. Die willen ze nog wel eens zelf installeren op zowel eigen apparaten als bedrijfsapparatuur. Allereerst moet dit legale software uit een betrouwbare bron zijn, om infecties en andere (juridische) problemen te voorkomen. Daarnaast is de kans groot dat medewerkers op eigen houtje bedrijfsgegevens naar deze tools overbrengen.

Maar aan het onderweg gebruiken van een openbaar netwerk kleven risico’s, omdat het netwerkverkeer eenvoudig is af te tappen.

In plaats van centraal opgeslagen, beveiligde en beheerde data, komt gevoelige bedrijfsinformatie nu ineens lokaal te staan. Met alle risico’s van dien. Het autorisatiemechanisme van de bedrijfsapplicatie wordt omzeild, zodat iedereen met toegang tot het lokale apparaat erbij kan. Er wordt waarschijnlijk geen back-up gemaakt en er is geen controle of de gegevens nog wel kloppen. Wordt het apparaat gestolen of verloren, dan valt data in handen van onbevoegden. Een mogelijke oplossingsrichting is de tools aanbieden via een virtuele desktop, zodat lokaal alleen nog een client nodig is.

Openbare netwerken

Altijd en overal werken heeft veel voordelen. Maar aan het onderweg gebruiken van een openbaar netwerk kleven risico’s, omdat het netwerkverkeer eenvoudig is af te tappen. Op die manier vallen gevoelige gegevens, gebruikersnamen, wachtwoorden en ip-nummers zo in handen van onbevoegden.

Een openbaar netwerk dat voor ons betrouwbaar lijkt kan ook nog eens een valstrik zijn. De netwerknaam kan namelijk de indruk wekken dat het om het netwerk van het vliegveld, restaurant of station gaat waarop we ons bevinden, terwijl het in werkelijkheid door de hacker is opgezet die met zijn laptop aan het tafeltje naast ons zit.

Voor bedrijven is het belangrijk dat ze nadenken of werken via een openbaar netwerk wel is toegestaan, en zo ja, welke werkzaamheden

via zo'n netwerk mogen worden gedaan. Voor extra veiligheid kan een vpn-tunnel worden opgezet. Het inrichten van extra accounts in een omgeving met beperkte bevoegdheden voor bijvoorbeeld alleen het raadplegen van data, kan een extra beveiligingsmaatregel zijn.

Social engineering

Als een medewerker van de it-afdeling belt met de vraag of we onze gebruikersnaam even willen doorgeven, of vraagt of we wel het juiste serveradres gebruiken, dan zijn wij uiteraard zeer behulpzaam. Maar hoe weet je of je wel echt met iemand van jouw bedrijf praat? Zeker in grotere organisaties ken je niet iedereen. Kwaadwillenden blijken er enorm goed in om via de telefoon of een e-mail vertrouwen te wekken. Via social engineering benaderen ze medewerkers en peuteren zo cruciale stukjes informatie los, om vervolgens een gerichte aanval uit te voeren. Vergelijk het met 'Microsoft' die particulieren belt en ze via enge meldingen in logbestanden overtuigt om software te installeren die alle problemen 'verhelpt'.

We zijn van nature geneigd om behulpzaam te zijn. Bewustwording dat dit soort vergaande trucs wordt uitgehaald om je te misleiden is cruciaal. Maak bijvoorbeeld bekend welke gegevens telefonisch mogen worden doorgegeven en welke alleen via persoonlijk contact.

Moedwillig

Een zeer ernstige categorie zijn medewerkers die moedwillig schade willen aanbrengen of op diefstal uit zijn. Zo kunnen ex-medewerkers vaak nog lang na uitdiensttreding vanaf afstand aanloggen omdat hun accounts niet geblokkeerd of verwijderd worden. Dat is een groot risico als iemand kwaad wil. Misschien leven er wraakgevoelens na een vertrek uit onvrede, of kan een ex-medewerker goede sier maken door gestolen informatie te gebruiken bij de nieuwe werkgever. Ook werknemers die elkaars gebruikersgegevens kennen of even een toegangspas lenen, kunnen onder andermans naam kwaad aanrichten zonder zelf tegen de lamp te lopen. Gebruikers met speciale accounts, zoals beheeraccounts of accounts met vergaande bevoegdheden in databases, hebben in het bijzonder veel mogelijkheden als ze kwade bedoelingen hebben.

Belangrijk is dat er toezicht is op de autorisaties die worden toegekend en dat er wordt gemonitord wie wanneer welke speciale accounts gebruikt. Ook helpt bewustwording en sociale controle op de werkvloer om mogelijke risico's sneller aan het licht te brengen.