avensus

Whitepaper

Zijn je medewerkers klaar om gehackt te worden?

Zo vergroot je het security-bewustzijn

Introductie

Een cyberongeluk zit tegenwoordig in een klein hoekje. Zowel organisaties als individuen doen steeds meer digitaal, terwijl cybercriminelen doorlopend betere trucs en technieken ontwikkelen om gaten te vinden in de cybersecurity verdediging van bedrijven en netwerken te penetreren.

Veel organisaties focussen zich bij het voorkomen van security-incidenten vooral op het technische aspect van beveiliging. Elk zichzelf respecterend bedrijf heeft inmiddels wel een firewall en goede antivirussoftware. Wat ze echter vaak vergeten is dat datalekken of ransom- en malwarebesmettingen in circa 90% van de gevallen toe te schrijven zijn aan menselijke fouten.

Een medewerker hoeft maar één keer op een kwaadwillende link te klikken of een mail met gevoelige informatie naar een verkeerde persoon te sturen, en het kwaad is geschied. Security-bewustzijn is dus minstens zo belangrijk als een goede technische security-structuur. In deze whitepaper laten we zien hoe je het security-bewustzijn onder medewerkers vergroot en tonen we hoe Avensus je daarbij helpt.

Waar het vaak misgaat

Een tekortschietend security-bewustzijn bij je medewerkers kan zich op verschillende manieren manifesteren. We geven je een overzicht van 7 veelgemaakte fouten die zwaarwegende gevolgen kunnen hebben.

Veelgemaakte fout 1:
Wachtwoorden

Gemak dient de mens. Maar er zijn uitzonderingen. Omdat we tegenwoordig veelal online werken, winkelen en ook onze financiële en verzekeringstechnische zaken via het internet regelen, dijt de lijst met wachtwoorden vaak stevig uit. Lastig om die allemaal te onthouden. Daarom gebruiken veel medewerkers jarenlang dezelfde wachtwoorden voor al hun accounts. Vaak maken ze daarbij ook geen onderscheid tussen privé-accounts en zakelijke accounts.

Dat is natuurlijk vragen om problemen. Word je wachtwoord gekraakt? Dan waant de hacker zich in een digitale goudmijn en kan hij bij al je accounts en data. Wat ook niet helpt is dat veel mensen een makkelijk te onthouden wachtwoord kiezen. Denk bijvoorbeeld aan klassieke wachtwoorden als **123456' of 'password'.** Maar wat makkelijk te onthouden is, is ook eenvoudig te raden. Tegenwoordig kan een hacker met verstand van zaken en de juiste apparatuur een simpel wachtwoord binnen enkele seconden of minuten kraken.

Veelgemaakte fout 2:
Zakelijke bestanden in de privémail

In de avonduren op je thuiscomputer nog even een belangrijke klus afmaken waar je overdag niet aan toe bent gekomen? En de vruchten van je arbeid versturen naar de privémail van de ontvanger? Het is vaak een recept voor problemen. Deze mailboxen zijn vaak lang niet zo goed beveiligd als de werkmail en dus ook eenvoudiger te hacken. Het zal je maar gebeuren dat een document met gevoelige persoonlijke of financiële informatie zo in de verkeerde handen belandt...

Veelgemaakte fout 3:
Geen meervoudige authenticatie

Het lekken van gebruikersnamen en wachtwoorden is nooit helemaal te voorkomen. Een techniek als meervoudige of 2-factor authenticatie (2FA), die nog minstens één andere authenticatiemethode vereist dan alleen een gebruikersnaam en wachtwoord, is dan ook een must in een moderne werkomgeving. Hoewel steeds meer bedrijven er gebruik van maken, is het nog niet binnen elke organisatie en voor elke medewerker een vanzelfsprekendheid.

Veelgemaakte fout 4:
Openbare netwerken

De aantrekkingskracht van plaatsonafhankelijk werken is groot. Hoe fijn is het als je jouw werk ook in het gezellige koffietentje om de hoek kunt doen? Het probleem is dat de openbare netwerken in zulke gelegenheden lang niet altijd goed beveiligd zijn. Hierdoor hebben hackers vaak volop mogelijkheden om digitaal in te breken op jouw laptop of smartphone. Zo kunnen ze data buitmaken of allerlei digitale deuren openzetten zonder dat je het in de gaten hebt.

Veelgemaakte fout 5:
Phishingmails

In de goede oude tijd waren phishingmails makkelijk te herkennen. Ze stonden vol taalfouten en kromme zinnen. Of ze kwamen van fictieve rijke baronnen of Nigeriaanse prinsen die je zonder aanwijsbare reden miljoenenschenkingen aanboden.

Tegenwoordig zijn phishingmails een stuk ingenieuzer en professioneler. Ze richten zich vaak op de actualiteit (corona of andere crises), zijn in vlekkeloos Nederlands of Engels opgesteld en herbergen vaak het niet van echt te onderscheiden logo en adres van een plausibele organisatie. Er hoeft maar één iemand op een link te klikken om mal- of ransomware toegang te geven tot je computer en netwerk, of de hacker een ingang te bieden naar een server met gevoelige informatie.

Veelgemaakte fout 6:
Je werkplek open en bloot achterlaten

Wat ook nogal eens gebeurt; medewerkers verzuimen om een document met gevoelige informatie af te sluiten of af te schermen als ze tijdelijk hun werkplek verlaten. Zo kan iedere willekeurige voorbijganger zien wat er op het scherm staat.

Veelgemaakte fout 7:
‘Wij worden niet gehackt’

‘Wij worden niet gehackt’ is een kreet die je nog te vaak hoort. Kleinere organisaties denken vaak dat ze geen doelwit zijn, terwijl grotere organisaties vaak (te) veel vertrouwen hebben in de techniek en de ‘softe’ kant van security onderschatten. In de praktijk is iedereen een potentieel doelwit en heb je weinig aan goede beveiligingstechniek zonder security-bewustzijn. Het laatste kun je vergelijken met rijden in een peperdure topwagen zonder rijbewijs.

Zijn je medewerkers klaar om gehackt te worden?

Gelukkig zijn er beproefde manieren om het security-bewustzijn binnen je organisatie naar een hoger niveau te tillen. En het goede nieuws is dat ze niet eens heel duur of complex hoeven te zijn. We delen er 5.

Manier 1:
Herhaling is het toverwoord

Herhaling is het toverwoord als het aankomt op security-bewustzijn. Veel organisaties bieden één keer per jaar een trainings- en phishingmodule aan en denken dat het dan voorlopig wel snor zit. Security-bewustzijn komt echter pas tot volle wasdom als cyberveiligheid een terugkerend iets is, een element dat verankerd is in de dagelijkse werkroutines van elke medewerker. Security-trainingen moeten dus niet eens per jaar, maar eigenlijk elke maand of ieder kwartaal op de bedrijfsagenda staan. Hetzelfde geldt voor pentests en vulnerability scans.

Manier 2:
Gedragsverandering afdwingen

Security-bewustzijn bovenaan de agenda krijgen is makkelijker als je het thema uit de sfeer van het vrijblijvende haalt. Verplicht medewerkers om security-trainingen te volgen en testen te doen. Neem dit ook op in de arbeidsvoorwaarden en koppel rollen en toegangsrechten van medewerkers of devices aan het 'awareness-niveau' van medewerkers. Haal je een test niet? Dan blijven bepaalde deuren even gesloten. Zo dwing je uiteindelijk gedragsverandering af.

Zorg ook voor sterke, lange wachtwoorden (die tenminste uit letters, hoofdletters en een paar andere tekens bestaan) en verplicht medewerkers om die eens in de zoveel tijd te veranderen. 2FA moet bovendien een vanzelfsprekendheid zijn. Stel ook duidelijke regels in voor het op afstand werken en koppel die aan het awareness-niveau van een medewerker.

"Security-trainingen moeten niet eens per jaar, maar eigenlijk elke maand of ieder kwartaal op de bedrijfsagenda staan."

Manier 3:
Maak het leuk en boeiend

Zorg ervoor dat security-trainingen aantrekkelijk en boeiend zijn. Bij Avensus gebruiken we bijvoorbeeld korte filmpjes in Netflix-stijl die het format hebben van een detective met een security-boodschap. Ook gamification biedt veel mogelijkheden om security-bewustzijn in een spannend en attractief jasje te steken. Denk bijvoorbeeld aan een spel waarin je security-tests koppelt aan levels en het spelen op tijd.

Manier 4:
Creëer een cultuur van vertrouwen

Een cultuur van vertrouwen is ook belangrijk als je een security-mindset wilt creëren. 100% veiligheid is een illusie. Maar het helpt wel als medewerkers weten bij wie ze moeten aankloppen als ze vermoeden dat er iets niet in de haak is. Zorg er bovendien voor dat je medewerkers niet direct aan de schandpaal nagelt als ze een fout maken. Als ze bang zijn voor bestraffing of bespotting zullen ze misschien niet melden dat ze op een link hebben geklikt of een bijlage hebben geopend.

Manier 5:
Blijf meten en geef inzicht

Meten is weten, ook als het aankomt op security-bewustzijn. Blijf altijd bijhouden waar je organisatie op enig moment staat. Wat is het actuele kennisniveau van medewerkers? Waar zitten nog gaten tussen kennis en actuele cyberdreigingen? Welk resultaat leveren bepaalde security-trainingen of -maatregelen concreet op? Neemt het aantal incidenten af? Door de antwoorden op die vragen in periodieke rapporten te gieten, zie je hoe het security-bewustzijn van medewerkers zich door de tijd ontwikkelt.

Hoe helpt Avensus?

Het awareness-platform van Avensus helpt bij het vergroten van het security-bewustzijn van jouw medewerkers. Dat doen we onder meer op de volgende manieren:

- Pentests, phishing tests en vulnerability scans. Deze worden uitgevoerd door ervaren technische consultants.
- Aantrekkelijke trainingsvormen, zoals boeiende detective fimpjes met een security-boodschap.
- Trainingen die thema's als phishing en het veilig beheren van devices en opslagmedia vanuit alle invalshoeken benaderen. We kijken dus niet alleen naar de klassieke mails, maar leggen bijvoorbeeld ook een USB-stick met malware op een parkeerplaats om te kijken wie hem opraapt en opent.
- Trainingen en praktijkvoorbeelden die we specifiek toespitsen op bepaalde lagen binnen je organisatie. Denk bijvoorbeeld aan aparte trainingen voor de directie, het management en de mensen op de werkvloer.

Meer weten?

Wil je het security-bewustzijn van je medewerkers een flinke boost geven? En ben je op zoek naar een partner die daarvoor de juiste methoden en tools in handen heeft? Neem dan gerust vrijblijvend contact met ons op via **+31 85 0200070** of **info@avensus.nl**.