Call script Websense

Pre-call

Voordat je begint met cold calling zijn er enkele zaken die je je moet afvragen:

- Welke persoon krijg ik aan de lijn?
    - **In welke branche is deze persoon werkzaam en wat zijn mogelijke branchespecifieke pijnpunten**? Denk aan regelgeving zoals NEN 7510 (zorgsector), Sarbanes-Oxley (beursgenoteerde bedrijven) en Basel III (financiële sector).
    - **Wat is de omvang van de organisatie**? Is het bedrijf nationaal of internationaal actief? Houd in het achterhoofd dat voor grote organisaties high availability een issue is en dat kleinere organisaties over het algemeen geen aparte security-afdeling hebben. Dit biedt mogelijkheden voor Websense.
    - **Welke functie heeft de persoon die je aan de telefoon krijgt**? Heeft hij/zij direct te maken met de problemen die je wilt adresseren en waar Websense een oplossing voor biedt?

      Tip: vraag bij enterprise accounts naar de Security Manager/Security Officer. Is er niemand met die functie? Vraag dan naar de IT-manager. Dit geldt ook voor kleinere organisaties. Onthoud dat de IT-manager over het algemeen meer beslissingsbevoegdheden heeft en dus de perfecte persoon is voor een afspraak.
    - **Welke verantwoordelijkheid heeft de persoon aan de andere kant van de lijn**? Een Security Manager heeft over het algemeen de volgende doelen:
        - **Terugdringen van de infrastructuurcomplexiteit**
        - **De overhead van change management verlagen**
        - **Beheer vereenvoudigen**
        - **Het niveau van beveiliging (ook mobiel!) verhogen**

Het gesprek

De belangrijkste doelstelling van het gesprek is:

Enterprise account

- Maken van een afspraak.
- Ideale gesprekspartner: Security Manager / IT-manager
    - Gespreksonderwerpen: terugdringen TCO, consolidatie, mobiele beveiliging en Data Loss Prevention (DLP).

Mkb en middensegment

- Inventariseren in hoeverre er een verkoopkans is voor Websense:
    - Is er budget?
    - Is er een behoefte binnen de organisatie waar Websense een oplossing voor biedt?
    - Op welke termijn moet deze behoefte worden ingevuld?
- Ideale gesprekspartner: IT-manager

Start van het gesprek

- Stel jezelf voor en vertel dat je belt namens security-specialist Websense.
- Als de persoon aangeeft dat je stoort, vraag je op welk moment je het beste terug kunt bellen. Noteer dit en bevestig nogmaals wanneer je weer contact opneemt.

- Mogelijke insteek met als doel het maken van een afspraak
    - Als je weet hoe groot het bedrijf is, kun je insteken op de huidige security-oplossingen die in gebruik zijn. “Volgens mijn gegevens werken bij uw organisatie ongeveer XX medewerkers. Dat betekent uitdagingen op het vlak van security: e-mail, data en wellicht mobiel. Graag zou ik met u een afspraak maken om te vertellen over de visie van Websense op security.”
    - Prospect kan zeggen: “Waarom?”
    - Antwoord: “Websense heeft een visie en bijbehorend portfolio waarmee uw organisatie grote voordelen realiseert.”
    - Prospect kan zeggen: “Welke voordelen dan?”
    - Antwoord: “Websense heeft een oplossing die web-, e-mail- en databeveiliging combineert en die u kunt beheren via één centrale console.

Een oplossing die ook nog eens de helft goedkoper is dan vergelijkbare producten. Onze oplossing – TRITON – combineert URL-filtering, antivirus, preventie van dataverlies, mobiele security, beveiliging van social media en proxybeveiliging."

- Prospect kan zeggen: "En wat levert mij dat op?"
- Antwoord: "U brengt de complexiteit van uw infrastructuur terug, verlaagt de overhead van change management, vereenvoudigt het beheer en verbetert de security – ook voor mobiele apparatuur en social media. Zullen we een afspraak maken zodat ik u de voordelen voor uw organisatie kan uitleggen?"
- Prospect kan zeggen: "Wie is Websense?"
- Antwoord: "Websense is een wereldwijde speler in web-, e-mail- en databeveiliging. We beveiliging geen losse onderdelen, maar al uw content: inkomende én uitgaande. Daarnaast zijn we de enige partij die één centrale beheersconsole biedt voor al deze beveiligingscomponenten. U bent dus beschermd tegen alle moderne bedreigingen zonder dat dit de complexiteit of beheerlast verhoogt. We combineren beveiliging bij u op locatie met oplossingen uit de cloud. Bovendien – en dat is in deze tijd belangrijker dan ooit – zijn onze oplossingen voordeliger dan die van de concurrentie én dringen ze infrastructuur- en beheerkosten terug. Daarover vertellen we u graag in een persoonlijk gesprek."
- Als de prospect nog steeds niet 'hapt', kun je vragen waarom hij/zij geen afspraak wilt maken. Het kost slechts een uur van hun tijd, maar zal hun kijk op security voorgoed veranderen.

Einde van het gesprek

- Bevestig altijd de afspraak: "Op [datum] komt om [tijdstip] iemand bij u langs. Hartelijk dank voor uw tijd." Of "Op [datum] om [tijdstip] neemt iemand van Websense contact met u op om een afspraak in te plannen."

Nadere kwalificatie beveiligingsbehoeften

Ga in op het TRITON-aanbod van Websense. Vraag naar de huidige situatie en behoefte per TRITON-component

- URL-filtering
- Antivirus
- preventie van dataverlies
- mobiele security
- beveiliging van social media
- proxybeveiliging

Tip: mogelijke vragen in het kort

- Wat staat er bij u op de agenda als het gaat om IT-security?
- Wat doet u op het vlak van mobiele beveiliging en BYOD?
- Welke projecten staan er op uw security-roadmap?
- Hoe staat u tegenover consolidatie?

Uitgebreid vragenoverzicht per TRITON component zie appendix A

Specifieke vragen en antwoorden

Cloud

- Prospect: “Wat doen jullie met de cloud?”
- Antwoord: “We zetten de cloud in om onze oplossingen op gehoste basis aan te bieden. Hierdoor profiteert u van maximale flexibiliteit en kostenefficiëntie.”
- Prospect: “Is mijn data wel veilig in de cloud?”
- Antwoord: “De Websense Cloudservice datacenters zijn voorzien van de hoogste ISO27001 certificering. Daarnaast voldoen wij aan alle privacy regelgeving binnen de EU. ”
- Hoe onderscheidend is Websense op dit gebied?
- Antwoord: “Wij zijn de enige partij met een echt hybride aanbod, met bijvoorbeeld een on premise oplossing voor het hoofdkantoor die communiceert met de cloud-oplossing voor roaming users.

Social media

- Prospect: “Wat doen jullie op het gebied van social media-beveiliging?”
- Antwoord: “Onze oplossingen monitoren social media-verkeer, maar daarin zijn we niet uniek. Waar we wel uniek in zijn, is onze realtime content classificatie. Wij bekijken alle componenten van bijvoorbeeld een Facebook-pagina, waaronder ook gaming, gokken en adult. Deze specifieke onderdelen van Facebook blokkeren we. Dit doen we uit het oogpunt van productiviteit en veiligheid. Websense is de enige partij die zo gedetailleerd monitort en beveiligt.”

Daarnaast hebben we een partnership met Facebook. Websense scant miljoenen links op Facebook per dag en classificeert deze en voert deze intelligentie terug naar het geavanceerde classificatie- en malware-identificatieplatform waar alle Websense gebruikers hun voordeel me doen.

Mobile

- Prospect: “Hoe beveiliging jullie mobiele data?
- Antwoord: “Met onze TRITON-oplossing beveiliging we web-, e-mail- én mobiel dataverkeer.”

Voordelen voor mijn organisatie

- Prospect: “Wat levert Websense mij financieel op?”
- Antwoord: “Buiten het feit dat onze oplossingen gemiddeld de helft kosten van vergelijkbare producten, dringt u de TCO van uw infrastructuur gemiddeld met maximaal veertig procent terug. De kosten voor beheer worden lager en u verkleint het risico op financiële schade door veiligheidsproblemen.”
- Prospect: “Hoe weet ik zeker dat alle voordelen die je schetst ook voor mijn organisatie gelden?
- Antwoord: “Tijdens het gesprek geven we openheid van zaken. We nemen uw kosten onder de loep en vertellen welke voordelen Websense u biedt. Websense is altijd volledig transparant. Als u daar prijs op stelt, kunnen we zelfs een proof-of-concept doen.”
- Prospect: “En waarom is Websense beter dan bedrijf X (concurrent)?”

- Antwoord: “Dat vertellen we u graag tijdens een kop koffie.”

BANT-kwalificatie

Budget

- Wat is het budget voor dit project?
- Wanneer wordt het budget vrijgegeven?

Authority

- Wat is uw rol in verband met het aftekenen van het budget en project?
- Wie zijn de andere partijen die te maken hebben met het aftekenen van het budget?

Need = Samenvatting van het gesprek

Timeline

- Wat is de timescale van de implementatie of tot wanneer denkt u dat jullie een beslissing genomen zullen hebben in verband met dit project?

<u>Tips</u>

- Als een organisatie meer dan 5.000 werknemers heeft, is de high performance next generation proxy een mooie insteek. Dit is een belangrijk issue in bedrijven met die omvang. Je kunt uitleggen dat de high performance next generation proxy een centraal beheer van de internettoegang binnen de hele organisatie biedt, throughput optimaliseert en uitgebreide cachingmogelijkheden biedt.
- Ga niet in discussie. Mocht iemand ‘lastige’ vragen stellen, geef dan aan dat je die graag beantwoordt in een persoonlijk gesprek.
- Heb je iemand aan de lijn die vraagt naar de technologie achter het Websense-aanbod (TRITON), vertel dan zeker over de ACE-engine.
    - ACE waakt over uw veiligheid door:

- dagelijks drie tot vijf miljard URL’s te analyseren;
- 99,999 procent van spam, phishing en schadelijke weblinks in e-mail tegen te gaan;

- patronen en onregelmatigheden te detecteren voor zero-day aanvallen.
    - ACE is voorzien van de nieuwste technologie, waaronder:
- realtime beveiligingsclassificatie;
- realtime contentclassificatie;
- Websense PreciseID-data-identificatie;
- antispam met 99 procent detectienauwkeurigheid*;
- reputatiediensten;
- webfiltering van het hoogste niveau;
- antivirus++.

APPENDIX A

WEB

Klantuitdaging	**Identificatie- en controlevragen**
Geavanceerde malware en gerichte aanvallen	-Hoe pakt u momenteel webbedreigingen aan en controleert u internettoegang? Wat werkt en wat niet? Welke impact heeft dit op uw bedrijf? - Welke beveiliging gebruikt u voor realtime analyse tegen gerichte aanvallen? -Welk beveiligingsmechanisme analyseert webpagina's, actieve scripts, links en bestanden in realtime? Om zo aanvallen tegen te gaan die gebruikmaken van dynamische levering, payloads en call home-methodes? -Kunt u beschrijven in hoeverre u in staat bent om een aanval tegen te houden voordat deze uw interne systemen besmet?
Datadiefstal/compliancy/regelgeving	-Hoe voorkomt u datadiefstal en -verlies bij internetgebruik? -Hoe beschermt u zich tegen diefstal van uitgaande data en call home-analyse? -Hoe detecteert uw huidige beveiligingsoplossing uitgaande, versleutelde bestanden, wachtwoorden, geolocaties of het gebruik van dynamische DNS?
Social media/networking/ medewerkerproductiviteit	-Hoe monitort u social media en zorgt voor u voor controle op het social media-beleid? -Hoe verzamelen uw huidige beveiligingsoplossingen beveiligingsintelligentie van Facebook of Twitter? -Hoe beoordeelt u of content ongewenst of contraproductief is? -Zouden tijdquota's en beleidscontrole op applicatiefuncties bij uw organisatie de productiviteit verhogen?
Te veel losstaande producten	-Op hoeveel systemen moet u inloggen om uw web-, e-mail- en databeveiligingssystemen te beheren of rapporteren?

	-Hoeveel apparaten (appliances, rapportageservers, beheerservers, encryptie-servers e.d.) heeft u nodig voor uw beveiligingsproducten voor web, e-mail en data? -Kun u uw beheerkennis gebruiken voor uw internetbeveiliging en deze ook benutten voor uw e-mail- en databeveiligingssystemen? -Wat gebeurt er als uw beveiligingsbeheerder op vakantie gaat? Zijn er binnen uw organisatie mensen die zijn of haar taken kunnen overnemen?

E-MAIL

Klantuitdaging	**Identificatie- en controlevragen**
Gemengde aanvallen die voorbijgaan aan de huidige beveiligingsoplossing	-Heeft u recentelijk te maken gehad met een incident op het gebied van e-mailbeveiliging? -Cybercriminelen maken steeds meer gebruik van gemengde aanvallen (e-mail- en webbedreigingen). Heeft u uw beveiliging hierop afgestemd? -Welke oplossing voor e-mailbeveiliging gebruikt u? En in hoeverre beschermt die oplossing u tegen de nieuwste bedreigingen, zoals spear-phishing-aanvallen in kleine volumes – aanvallen die e-mail- en webkwetsbaarheden gebruiken om gevoelige data te stelen? Maakt de oplossing gebruik van historische reputatie van IP- en webadressen of webpagina's?
Verlies van medewerkerproductiviteit	-Hoe hoog is het percentage spam binnen uw bedrijf? Hoeveel daarvan houdt uw bestaande oplossing tegen? Weke SLA's heeft u voor het detecteren van malware en spam? -Hoe reageert uw bestaande e-mailinfrastructuur op een sterke groei in spam/e-mailverkeer? -Wat gebeurt erbij een netwerk- of mailserverstoring? Hoe voorkomt u dat e-mails verloren gaan?

Juridische risico's	-Aan welke regelgeving moet u voldoen? -Hoe bepaalt u momenteel of gevoelige data via e-mail de organisatie verlaat? -Heeft u te maken gehad met datalekken of -diefstal in het afgelopen jaar?
Te veel losstaande producten	-Op hoeveel systemen moet u inloggen om uw web-, e-mail- en databeveiligingssystemen te beheren of rapporteren? -Hoeveel apparaten (appliances, rapportageservers, beheerservers, encryptie-servers e.d.) heeft u nodig voor uw beveiligingsproducten voor web, e-mail en data? -Kun u uw beheerkennis gebruiken voor uw internetbeveiliging en deze ook benutten voor uw e-mail- en databeveiligingssystemen? -Wat gebeurt er als uw beveiligingsbeheerder op vakantie gaat? Zijn er binnen uw organisatie mensen die zijn of haar taken kunnen overnemen?

DATA

Klantuitdaging	**Identificatie- en controlevragen**
Toenemende druk om social media, cloud en mobiel toe te staan	-Welke websitetypes beschouwt u als de grootste bedreiging voor dataverlies? Wat doet u momenteel om dat risico terug te dringen? -Welke mobiele apparatuur ondersteunt u momenteel of bent u van plan te ondersteunen in de toekomst? Wat is volgens u het grootste risico van mobiele apparatuur voor uw bedrijf? -Welke cloud-diensten gebruikt u? Wat doen de leveranciers van die diensten om u te beschermen tegen dataverlies en -diefstal? Wat vindt u daarvan?
Niet in staat om te bepalen wanneer gevoelige	-Op welke manier identificeert u wanneer data risico loopt? Hoe effectief is de nauwkeurigheid daarvan? Heeft u te maken met veel false positives?

informatie risico loopt	-Welke kanalen zijn volgens u het gevaarlijkst voor dataverlies? -Welk gedrag van uw medewerkers brengt het grootste risico op dataverlies met zich mee? -Hoe groot is de kans dat gevoelige informatie op gefaxte en gescande documenten staat?
Angst voor datadiefstal	-Onderzoek van Websense Security Labs wijst uit dat 39 procent van de malware op het internet code omvat voor het stelen van data. En dit percentage groeit, ook op bijvoorbeeld mobiel. Hoeveel zorgen maakt u zich hierom? -In hoeverre denkt u dat uw huidige oplossing interne datadiefstal kan detecteren en hierop kan inspelen? -Welke informatie zou de meeste impact hebben op uw bedrijf als deze wordt gestolen?
Regelmatige audits en onderzoek	-Hoe denkt u DLP in te kunnen zetten om te voldoen aan regelgeving? Hoe verschilt dit van uw huidige situatie? -Hoeveel mensen zijn betrokken bij de voorbereidingen op een audit? Hoeveel tijd neemt dit proces in beslag? -Zijn verschillende mensen/groepen verantwoordelijk voor data-governance in hun regio? Hoe worden zij betrokken bij het beslisproces? -Waarom is het voor u persoonlijk belangrijk dat u beschikt over krachtig beleid op dit vlak?

MOBILE

Klantuitdaging	**Identificatie- en controlevragen**
Onbeveiligde mobiele apparatuur op kantoor	-Mogen uw medewerkers persoonlijke mobiele apparatuur gebruiken voor hun werk? -Hoeveel mobiele apparaten hebben toegang tot uw bedrijfsnetwerk? -Wat is uw belangrijkste angst als het gaat om privéapparatuur die

	toegang heeft tot uw bedrijfsnetwerk? -Wat doet u om deze apparatuur te beveiligen en bedrijfsdata te beschermen?
Malware en geïnfecteerde mobiele apps	-Hoe beschermt u mobiele gebruikers tegen malware, dataverlies en apparaatverlies? -Welke oplossing gebruikt u momenteel om data op mobiele apparatuur te beschermen tegen diefstal? Werkt deze oplossing? -Hoe brengt u in kaart welke mobiele apps via uw netwerk worden gedownload naar apparatuur? -Hoe bepaalt u of nieuwe of geüpdatet apps schadelijke content bevatten? -Wat is uw beleid als het gaat om smartphones of tablets die zijn gejailbreaked?
Data Loss Prevention (DLP)	-Maakt u zich zorgen dat gevoelige informatie lekt van mobiele apparatuur buiten uw organisatie? -Hoe beschermt u gevoelige informatie op uw netwerk tegen toegang via mobiele apparatuur? -Kunt u een limiet stellen aan de hoeveelheid of het type data dat wordt benaderd via mobiele apparatuur?