PHISHINGMAILS VERMOMD ALS DIEETWENSENLIJST OF KLACHTENBRIEF

Van administratie tot directie, iedereen leert over de nieuwste cybertrucs

Bij de meeste bedrijven wordt maar liefst 70 procent van alle veiligheidsincidenten veroorzaakt door menselijke fouten. Bij hotels is dat niet anders. WestCord Hotels wil er alles aan doen om te voorkomen dat gastgegevens op straat komen te liggen. Daarom volgt het personeel een Security Awareness training. Johannes van der Kooi en Maurits Bots vertellen hoe deze training WestCord Hotels kan beschermen.

Een poging tot oplichting begint allang niet meer met een slecht geschreven e-mail van een vage bekende die je veel geld belooft als je nu duizend dollar overmaakt. De nieuwste phishingmails zijn vele malen gewiekster, vertelt Maurits Bots, IT-specialist bij WestCord Hotels. “Criminelen personaliseren hun phishingmails, net zoals de afdeling marketing e-mails aan relaties personaliseert. Daardoor lijkt een e-mail die zogenaamd van een gast komt net echt.” Cybercriminelen weten precies hoe ze in de hotelwereld de aandacht moeten trekken. Ze sturen bijvoorbeeld een mail over een klacht of over dieetwensen met een link naar een bestand. “Dat lijkt een plausibel verhaal, maar er moet dan toch een belletje gaan rinkelen. Daarom nemen we onze medewerkers mee in deze wereld, om hen weerbaarder te maken tegen dit soort incidenten. Wij zijn nog geen slachtoffer geworden, maar voorkomen is beter dan genezen.”


Maurits Bots en Johannes van der Kooi


Hotel Arsenaal Delft by WestCord

ss Rotterdam by WestCord

SCHADE VOOR DE GAST

De gevolgen van een klik op een fout bestandje of een misleidende link kunnen desastreus zijn. Maurits: “Als er één computer besmet raakt met malware, is dat voor ons nog niet zo erg. Ons systeem is zo ingericht dat die pc onmiddellijk wordt geblokkeerd. Maar het kan ook gebeuren dat een medewerker een wachtwoord invult om toegang te krijgen tot een bestand of website. Als hij of zij datzelfde wachtwoord ook voor andere systemen gebruikt, bijvoorbeeld voor een boekingssite, dan is de kans levensgroot dat onze gastgegevens op straat liggen.”
Gastgegevens zijn de meest kwetsbare data van een hotel. Namen, adressen en gevoelige gegevens als creditcard- en bankrekeningnummers horen goed beschermd te zijn. Datalekken kunnen leiden tot schade voor de gast en de Autoriteit Persoonsgegevens kan het bedrijf een boete opleggen. Het is dus erg belangrijk om incidenten te voorkomen. Maar dat is nog niet zo makkelijk met 1600 medewerkers, van wie een groot deel op de één of andere manier te maken heeft met e-mailverkeer en computergebruik, zegt hospitality trainer Johannes van der Kooi. “Zelfs telefonische reserveringen kunnen gevaarlijk zijn. Soms probeert iemand telefonisch vertrouwen te wekken door een reservering te maken en stuurt daarna een phishingmail.”

TRAINING IN ACHT TALEN

Om te voorkomen dat medewerkers in de geraffineerde misleiding van cybercriminelen trappen, ging WestCord Hotels op zoek naar een laagdrempelige online training die begrijpelijk is voor iedereen. Johannes: “Maurits en ik hebben verschillende demo-accounts bekeken. Onafhankelijk van elkaar kwamen we uit bij de Security Awareness training van VSA. Die laat simpele voorbeelden van cybercriminaliteit zien in humoristische animaties. De bad guys hebben een zwart masker op en een computervirus ziet eruit als een coronavirus. Maar zo’n simpel filmpje is wel in staat om mensen aan het denken te zetten.” Medewerkers kunnen de training volgen in acht talen, waaronder Pools of Tsjechisch. Ze krijgen een link die ze kunnen openen op hun computer, tablet of telefoon, waar en wanneer ze maar willen. Ze hebben twee weken de tijd om de training te volgen. Daarna krijgen ze weer een nieuwe link.

“OH, KAN DAT OOK?!”

WestCord Hotels is een keten van 17 hotels. De general manager van ieder hotel zorgt ervoor dat iedereen die dat nodig heeft de training volgt. Johannes: “Dat is in ieder geval iedereen die dagelijks een muis gebruikt, dus backoffice, frontoffice en administratie, maar ook alle afdelingshoofden en de directie. De general manager kan ook extra personeelsleden uitnodigen, bijvoorbeeld medewerkers die uit enthousiasme graag gasten te woord staan.” In totaal volgen 571 medewerkers de training.” Personeelsleden die geld kunnen overmaken volgen nog een extra verdieping, waarin ze leren CEO-fraude te herkennen. Bij CEO-fraude krijgt iemand een verzoek om geld over te maken, schijnbaar van een bekende. Johannes: “Ook van general managers horen we terug dat ze de modules met open mond volgen. En dat ze voorbeelden zien waarbij ze denken: Oh, kan dat ook?!”

AI EN STEMVERVORMING

Cybercriminaliteit verandert snel en steeds weer duiken er nieuwe en slimmere trucs op. Met de opmars van AI zal dat alleen maar erger worden, weet Maurits. “Vroeger kregen we nog wel eens een bericht in slecht Engels dat zogenaamd van de directie kwam, maar nu zijn de mails soms niet van echt te onderscheiden. Ook stemvervorming wordt steeds beter, dus als iemand belt kun je er niet zomaar van uitgaan dat iemand is wie hij zegt dat hij is.” Johannes vult aan: “We willen uitgaan van het goede van de mens, maar dat kan niet meer. In de hotellerie voelt dat als behoorlijk tegenstrijdig. Vroeger controleerden we alleen of een naam in ons systeem voorkwam voordat we een vraag beantwoordden. Nu moeten we wantrouwender zijn. Met de Security Awareness training hebben we voor een heel jaar content beschikbaar om iedereen scherp te houden. Aan de hand van testresultaten monitoren we welke onderwerpen extra aandacht nodig hebben. Zo doen we er alles aan om te voorkomen dat WestCord Hotels slachtoffer wordt.”

VSA Security Awareness training

Wilt u meer weten? Neem dan contact op via
+31 (0)88 872 0 530 of security@vsa.nl