imprivata®

Het C-Suite strijdplan voor cyberbeveiliging in de zorgsector

"Als je de vijand én jezelf kent, kun je honderd veldslagen met vertrouwen tegemoetzien."
– Sun Tzu, De kunst van het oorlogvoeren

Volgens nieuwe wetgeving riskeren zorgorganisaties vanaf 1 januari 2016 een boete tot 860.000 euro wanneer ze nalaten een datalek te melden bij het College Bescherming Persoonsgegevens (CBP).

Technologie ligt ten grondslag aan de moderne samenleving en cyberbeveiliging is een belangrijk slagveld voor hedendaagse zorgorganisaties. Informatie is een van uw waardevolste bezittingen en criminelen doen er alles aan om deze in handen te krijgen.

Bij het leveren van goede patiëntenzorg moeten zorginstellingen de medische informatie en de patiëntengegevens zowel binnen als buiten het elektronische patiëntendossier goed beschermen. Naarmate er meer patiëntendossiers worden uitgewisseld en toegevoegd, nemen de potentiële risico's toe. Het Landelijk Schakelpunt[1] maakt de veilige uitwisseling van gestandaardiseerde medische gegevens mogelijk tussen zorgverleners zoals huisartsen en apotheken (uitsluitend na expliciete toestemming van de patiënt). Het is bekend wat er verkeerd kan gaan als de beveiliging ontoereikend is, zoals bij de hack van het Groene Hart Ziekenhuis in 2012, waarbij honderdduizenden patiëntendossiers werden gelekt[2]. Het Nederlands Normalisatie-instituut heeft de norm NEN 7510 'Informatiebeveiliging in de zorg'[3] ontwikkeld. Het Ministerie van Volksgezondheid, Welzijn en Sport (VWS) heeft de rechten op NEN 7510 (en de bijbehorende normen NEN 7512 en 7513) aangekocht, zodat deze gratis toegankelijk zijn en alle zorgorganisaties de veiligheidsmaatregelen kunnen implementeren en zelfs (delen van) de organisatie kunnen laten certificeren.

Regelen vóór 1 januari 2016

De druk neemt toe. Met ingang van 1 januari 2016 zijn Nederlandse bedrijven en organisaties (inclusief zorginstellingen en andere organisaties in de zorgketen) die met persoonsgegevens werken, wettelijk verplicht om datalekken onmiddellijk te melden bij het College Bescherming Persoonsgegevens (CBP). Na melding van een incident heeft de organisatie 72 uur om het lek te dichten. Als de organisatie hier niet in slaagt, of als een datalek niet wordt gemeld, kunnen boetes tot een hoogte van 860.000 euro worden opgelegd. Daarnaast krijgen topmanagers en CISO's een persoonlijke aansprakelijkheid.[4]

De belangrijkste zwakke plek in de meeste IT-beveiligingssystemen wordt gevormd door de wachtwoorden van de medewerkers. Deze veroorzaken een spanningsveld tussen veiligheid en efficiëntie. Wachtwoorden kunnen zelfs aan gemotiveerde en hoogopgeleide klinische of administratieve medewerkers worden ontfutseld door middel van phishing-aanvallen, waarvan sommige zo geraffineerd zijn geworden dat ze vrijwel niet tegen te houden zijn. NEN 7510 schrijft voor dat alle specialisten en zorgverleners moeten inloggen met hun eigen naam en hun persoonlijke wachtwoord, in plaats van gebruik te maken van groepsaccounts. De norm adviseert ook de inzet van oplossingen voor sterke wachtwoorden, wachtwoordbeheer-selfservice, sessie-timeouts en tweeledige authenticatie. Identiteitsbeheer en toegang op basis van rollen spelen een belangrijke rol in de NEN-beveiligingsnorm.

1. https://www.vzvz.nl/page/ICT-leverancier/Het-LSP
2. http://www.nu.nl/binnenland/2927832/groene-hart-ziekenhuis-lekt-medische-dossiers.html
3. https://www.werkenmetnen7510.nl/normen
4. https://cbpweb.nl/nl/melden/meldplicht-datalekken, of download vanaf de Imprivata-website het witboek "Een datalek voorkomen is beter dan genezen" door Duthler Associates en First Lawyers

Uw verdedigingsplan

"Gebruik tweeledige authenticatie of overweeg wachtwoord-beheersoftware; gewone wachtwoorden zijn niet veilig".

- Nationaal Cyber Security Centrum, Ministerie van Veiligheid en Justitie[5]

Deze NEN-norm is niet verplicht, maar de informatiebeveiliging valt onder supervisie van de Inspectie voor de Gezondheidszorg (IGZ), die het niveau van de beveiligingsmaatregelen bij zorgverleners beoordeelt aan de hand van NEN 7510.

Dit witboek biedt CCIO's en IT-beveiligingsmanagers in de gezondheidszorg de benodigde management- en technologiestrategieën om zwakke plekken rond wachtwoorden te kunnen bestrijden. Bovendien vindt u hier tools om de sociale gewoonten van klinisch personeel beter te begrijpen en te versterken, omdat hackers met veel succes misbruik maken van bepaalde aspecten van deze gewoonten.

Ken uw vijand

IT-managers en CCIO's in de zorg hebben met bewonderenswaardige snelheid gereageerd op de recente reeks inbreuken op de informatiebeveiliging: ondanks beperkte middelen hebben ze de verdediging van de netwerkperimeter versterkt, en ze zijn veel scherpere eisen gaan stellen aan wachtwoordbeveiliging. Veel organisaties hebben versterkte perimeters aangelegd die bestand zijn tegen krachtige DDoS-aanvallen (Distributed Denial of Service) en andere aanvallen met een hoge impact.[6]

Dergelijke maatregelen hebben echter weinig zin als CCIO's zich niet bewust zijn van de harde werkelijkheid: niet de toegangspoort, maar de poortwachter zelf is tegenwoordig het meest waarschijnlijke doelwit van een aanval. Uw medewerkers zijn de poortwachters van uw verdedigingsmechanismen en vormen het meest kwetsbare element van uw IT-beveiliging. Volgens IBM speelt dit probleem in een groot aantal sectoren en specialismen[7]. Niets menselijks is uw medewerkers vreemd: het zijn immers mensen die gebruikmaken van wachtwoorden. Hun wachtwoorden zijn de sleutels tot de toegangspoorten in uw perimeter en deze sleutels kunnen gemakkelijk gestolen worden door middel van social engineering-methoden die zich richten op de minst beheersbare aspecten van het menselijk gedrag.

De medische dossiers van patiënten zijn op de zwarte markt tegenwoordig meer waard dan gestolen creditcardnummers[8]. Dit gegeven leidt tot ongekend hoge aantallen frauduleuze verzekeringsclaims, gevallen van identiteitsdiefstal en cyberaanvallen op zorgorganisaties. Als leider op het gebied van zorgtechnologie hebt u behoefte aan geavanceerde verdedigingsstrategieën om de data van uw zorgorganisatie te beschermen tegen aanvallen. Het vereist zowel IT- als managementexpertise om de gegevensbeveiliging in balans te brengen met een hoge productiviteit.

Hoe gemotiveerd of intelligent uw medewerkers ook zijn, ze kunnen via steeds geraffineerdere aanvallen gemakkelijk worden gemanipuleerd om hun wachtwoorden prijs te geven. Het is een klassiek verhaal: zoals de Chinese Muur voortdurend werd geïnfiltreerd doordat wachters hun plicht

5. https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/factsheets/factsheet-use-two-factor-authentication/1/Factsheet%2BUse%2Btwo%2Bfactor%2Bauthentication.pdf
6. De drie gebieden waaraan het meeste geld wordt uitgegeven na een datalek zijn het beheer van beveiligingsincidenten, eindpuntbeveiliging en inbraakdetectie en -preventie, volgens het Ponemon Report 2014: A Year of Mega Breaches, http://www.ponemon.org/local/upload/file/2014%20The%20Year%20 of%20the%20Mega%20Breach%20FINAL_3.pdf
7. IBM: Quantifying the data breach epidemic, http://www-935.ibm.com/services/uk/en/it-services/data-breach/data-breach-statistics.html
8. Caroline Humer & Jim Finkle: Your medical record is worth more to hackers than your credit card, http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

verzaakten, en zoals de muren van Troje uiteindelijk vielen door het Griekse bedrog met het Paard van Troje, zo worden uw medewerkers het slachtoffer van goed verhulde aanvallen die misbruik maken van hun vertrouwen. Phishing-, spearphishing- en whaling-aanvallen richten zich op individuele zorgverleners of administratieve medewerkers. Bij deze aanvallen worden medewerkers via nagemaakte e-mails van IT-beheerders, nagebootste EPD-vensters of vervalste upgradepakketten gemanipuleerd om hun wachtwoorden prijs te geven.

Vaak is één enkele muisklik of één ingevoerd wachtwoord al voldoende om de beveiliging van een hele zorginstelling op de knieën te krijgen. Zoals blijkt uit de legende over het Paard van Troje (en uit de recente Anthem-aanval[9]), is de kracht van uw perimeter minder essentieel dan de beveiliging van uw toegangspoorten, en dan met name de zorgvuldigheid waarmee uw poortwachters hun sleutels beheren. De muren van Troje hadden 10 jaar fier stand gehouden – totdat de Grieken hun toevlucht namen tot social engineering.

In dit witboek kijken we naar de meest voorkomende menselijke oorzaken van zwakke plekken in het wachtwoordbeheer die de netwerkperimeter van zorgorganisaties kwetsbaar maken. Deze informatie is bedoeld om IT-beveiligers te helpen deze zwakheden in kaart te brengen, te begrijpen en om te vormen tot sterke punten door middel van een eenvoudige strategie die zowel door militaire leiders als door hackers wordt gevolgd: ken de vijand en ken jezelf. Want als het gaat om de beveiliging van uw zorginstelling, vormt uw eigen organisatie de grootste zwakheid: één verkeerde actie door één enkele medewerker kan uw hele bedrijfsvoering in gevaar brengen.

Ken uzelf

De beste aanpak bij het beschermen van uw zorginstelling tegen aanvallen op medewerkerswachtwoorden is het observeren van uw organisatie vanuit het perspectief van de hacker. Hackers doen grondig onderzoek voordat ze hun prooi aanvallen. Soms observeren ze wekenlang het digitale gedrag van gebruikers, voordat ze besluiten welke route de meeste kans op een succesvolle social engineering-aanval biedt. De hackers proberen hun doelwitten zo goed mogelijk te begrijpen, zodat ze hen kunnen verleiden hun geheimen prijs te geven. Proactieve IT-beveiligers doen hetzelfde: ze evalueren zorgvuldig de zwakke plekken in de organisatie, de problemen in workflows en de culturele aspecten, en daarna ontwikkelen ze de optimale verdedigingsstrategie. Deze aanpak bestaat uit de volgende stappen:

- In kaart brengen van de meest waarschijnlijke aanvalsmethoden: de belangrijkste gedragingen van medewerkers en andere risicofactoren.
- Begrijpen waardoor de zwakke plekken worden veroorzaakt: de vereisten van de workflows en andere factoren die ertoe bijdragen dat uw klinisch en administratief personeel geneigd is tot riskant gedrag.
- De oorzaken van de zwakke plekken elimineren: terugdringen van riskant gedrag via technologische en/of sociale maatregelen.

De beste aanpak bij het beschermen van uw zorgorganisatie tegen aanvallen op medewerkerswacht-woorden is het observeren van uw organisatie vanuit het perspectief van de hacker.

9. Voor meer informatie over de cruciale rol die het gestolen paspoort van een medewerker speelde bij de Anthem-hack, zie http://www.fiercehealthit.com/story/details-emerge-anthem-hack/2015-02-06

Om de risico's van diefstal van apparaten te verkleinen, schakelen veel organisaties in de zorg over op virtuele desktopsystemen (VDI) met thin clients en zero clients.

Breng de meest waarschijnlijke aanvalsmethoden in kaart

De meest voorkomende strijdplannen

Medewerkers vormen de zwakste schakel in de IT-beveiliging van een organisatie. Juist in de gezondheidszorg ontstaan heel veel zwakke plekken door het wachtwoordgedrag van medewerkers, door trucs om in- en uitloggen te vermijden en door het gemak waarmee medewerkers in dialoogvensters klikken of e-mails openen. Deze risico's doen zich voor in uiteenlopende situaties, waarvan aanvallers op specifieke manieren misbruik proberen te maken. Dit zijn de meest voorkomende aanvalsmethoden:

Phishing

Phishing is de verzamelnaam voor misleiding via elektronische communicatie (meestal e-mail) om gebruikersgegevens, wachtwoorden, creditcardnummers of andere gevoelige informatie in handen te krijgen.

Spearphishing

Spearphishing is een op één persoon gerichte vorm van phishing, waarbij oplichters proberen informatie te verkrijgen door nagemaakte e-mails te versturen die op het eerste gezicht afkomstig zijn van mensen of bedrijven die het slachtoffer kent of vertrouwt. Spearphishing berust op vertrouwdheid en vertrouwen van persoonlijke en zakelijke relaties.

Whaling

Whaling is een vorm van spearphishing die zich richt op 'grote vissen': topmanagers en andere verantwoordelijken die op hoog niveau toegang hebben tot de computersystemen van hun organisatie. Populaire doelwitten zijn CCIO's, IT-managers, EPD-beheerders en niet-technische topmanagers.

Zoekgeraakte of gestolen apparatuur

Verlies en diefstal van laptops en mobiele apparaten veroorzaken nog steeds grote risico's voor zorgorganisaties die hierop gevoelige informatie opslaan. Dit is een toenemende trend nu steeds meer zorginstellingen een BYOD-beleid gaan hanteren (Bring Your Own Device). Om de risico's van diefstal van apparaten te verkleinen, schakelen veel zorgorganisaties over op virtuele desktopsystemen (VDI) met thin clients en zero clients.[10]

Wachtwoordlijsten die niet versleuteld zijn

Medewerkers die moe worden van de vele wachtwoorden die ze moeten onthouden, bewaren vaak niet-versleutelde tekstbestanden met al hun wachtwoorden op een computer. Ze plakken zelfs briefjes met voor iedereen zichtbare applicatiewachtwoorden op een toetsenbord of beeldscherm. Volledige encryptie van harddisks helpt de risico's van niet-versleutelde wachtwoorddocumenten te verkleinen, maar er is geen kruid gewassen tegen de zwakke plek die Post-it heet.

10. Volgens het Imprivata-rapport Desktop Virtualization Trends in Healthcare 2014 geeft 84% van de ondervraagden aan dat hun organisatie de komende 24 maanden gebruik zal maken van SSO binnen hun VDI-omgeving. Zie http://pages.imprivata.com/rs/imprivata/images/Imprivata-2014-Desktop-Virtualization-Trends-in-Healthcare-Report.pdf

Test uw eigen beveiliging
Sommige IT-teams voeren interne 'penetratietests' uit, waarbij ze de strategieën van hackers nabootsen[11]. De resultaten zijn vaak weinig geruststellend. Uit gesprekken van Imprivata met IT-managers van toonaangevende zorginstellingen blijkt dat minstens 30% van deze penetratiepogingen slaagt. Vergelijkbare resultaten worden gemeld door McAfee. De resultaten van hun Phishing Quiz-test geven aan dat 80% van de 16.000 zakelijke gebruikers die zij via phishing probeerden te misleiden, minimaal één keer in de val trapten[12]. Daarnaast bleek uit het onderzoek van McAfee dat de slechtst scorende medewerkers vaak werken op afdelingen met veel gevoelige informatie (financiën, HR). Deze medewerkers hebben soms niet veel IT-kennis of zijn onvoldoende gemotiveerd.

Dit zijn schokkende resultaten, aangezien één enkele fout door een medewerker al genoeg kan zijn om de beveiliging van de zorgorganisatie te doorbreken. Ongeacht de uitkomsten van uw interne penetratietest, blijkt dit een zeer nuttige exercitie te zijn: u krijgt waardevolle inzichten in de gevoeligheid voor specifieke soorten aanvallen die op uw medewerkers zijn gericht. Hierdoor kunt u zien of er extra strategische maatregelen nodig zijn voor bepaalde afdelingen, applicaties of klinische workflows.

De resultaten van de McAfee Phishing Quiz laten zien dat 80% van de 16.000 onderzochte zakelijke gebruikers zich bij een test heeft laten misleiden door minimaal één phishing-poging.

Analyseer de oorzaken van zwakke plekken in uw organisatie

Het is niet voldoende te weten wát uw zwakke plekken zijn. Om de zwakke plekken te kunnen verhelpen, moet u ook begrijpen waardoor ze worden veroorzaakt. Het is belangrijk dat u de oorzaken van riskant werknemersgedrag kent, zodat u uw organisatie hiertegen kunt beschermen. Dit zijn enkele van de meest voorkomende oorzaken in de zorgsector:

Te veel wachtwoorden
Vaak is de oorzaak van veiligheidslekken door wachtwoorden duidelijk: zorgverleners hebben teveel wachtwoorden en moeten deze te vaak invoeren. Het wordt dan een automatisme om een wachtwoord in te typen zodra hier in een venster om gevraagd wordt. Bovendien kunnen medewerkers in een stressvolle klinische omgeving gefrustreerd raken wanneer er verschillende wachtwoordregels gelden voor verschillende applicaties of binnen een andere context. De ergernis neemt nog verder toe indien er wordt gewerkt met verouderde of trage systemen. Deze regels leiden ook vaak tot het delen en op meerdere plaatsen gebruiken van wachtwoorden: ideale omstandigheden voor hackers. Hoewel steeds meer zorginstellingen geavanceerde systemen met meervoudige authenticatie invoeren om de wachtwoorddruk te verminderen, zal de druk op medewerkers toch nog verder oplopen door het toenemende gebruik van SaaS-applicaties.

11. Voor meer informatie en advies over penetratietests, zie http://www.sans.org/reading-room/whitepapers/testing/ penetration-testing-alternative-password-cracking-35717
12. McAfee Labs Threats Report, augustus 2014, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2014.pdf

In een omgeving met gedeelde werkstations voelen medewerkers zich niet verantwoordelijk voor specifieke computers.

Te weinig kennis
Vaak realiseren zorgverleners zich niet hoe doelgericht en goed gecamoufleerd hackingaanvallen kunnen zijn. Vooral klinische medewerkers zijn zich vaak niet bewust van de groeiende risico's, omdat ze voortdurend in beslag worden genomen door de patiëntenzorg, met spoedbehandelingen en andere situaties die snelle beslissingen vereisen. De patiëntenzorg heeft uiteraard de hoogste prioriteit. De meeste medewerkers zullen niet gauw klikken op een link in een verdachte e-mail van een buitenlandse prins of een sjeik, maar ze zijn zich minder bewust van de risico's van malware, Trojaanse paarden of spearphishing-aanvallen die op het oog afkomstig zijn van een lokale, bekende afzender.

Te veel om te onthouden
Een gemiddelde zorgverlener heeft tientallen verschillende, complexe wachtwoorden nodig om in te loggen op EPD-systemen en klinische applicaties. Al deze wachtwoorden zijn vaak complex en moeilijk te onthouden als gevolg van strikte voorschriften. Veel medewerkers willen voorkomen dat hun account wordt geblokkeerd omdat ze een wachtwoord vergeten zijn, en ze noteren hun wachtwoorden daarom in notitieboekjes, agenda's of niet-versleutelde Word-bestanden of op plakbriefjes op hun computer.

Te veel mensen
Gedeelde werkstations zijn een alledaags verschijnsel in de zorg en steeds meer zorginstellingen schakelen over naar virtuele desktopsystemen (VDI). In een dergelijke omgeving voelen medewerkers zich niet verantwoordelijk voor specifieke computers. Hierdoor is ook de verantwoordelijkheid voor de controle op de beveiligingsinstellingen niet eenduidig. Bovendien groeit het risico dat mensen accounts gaan delen of dat ze per ongeluk de instellingen van anderen overschrijven. En ten slotte neemt het aantal in- en uitlogacties exponentieel toe.

Te weinig tijd
Soms hebben klinische medewerkers domweg geen tijd om uit te loggen wanneer ze plotseling worden weggeroepen voor een spoedgeval, of om goed te kunnen beoordelen of een wachtwoordvenster wel legitiem is terwijl ze een dringende medische handeling verrichten. Klinisch personeel werkt onder hoge tijdsdruk in een zeer stressvolle werkomgeving. Medewerkers delen vaak wachtwoorden met hun collega's om minder te worden gehinderd door de extra complexiteit die de IT-beveiliging toevoegt aan hun vele andere verantwoordelijkheden.

Vaak blijven ze ingelogd wanneer ze een werkstation verlaten, omdat het eindeloze in- en weer uitloggen teveel tijd kost en ten koste gaat van de patiëntenzorg.

Elimineer de oorzaken van zwakke plekken in uw organisatie

Nadat u de belangrijkste oorzaken van het riskante gedrag van uw medewerkers in kaart hebt gebracht, kunt u technologische maatregelen nemen om deze zwakke plekken te versterken. U kunt uw systemen zodanig aanpassen dat de huidige zwakke plekken minder vatbaar worden voor misbruik. Mogelijk kunt u de zwakke plekken zelfs geheel elimineren door het gedrag van uw mensen te wijzigen via doelgerichte technologische maatregelen en trainingen die oplossingen bieden voor de problemen met de huidige processen.

Omdat medewerkers in de zorg op vele manieren gevoelig zijn voor aanvalspogingen, kan de beveiliging niet alleen door middel van gebruikerstrainingen worden gewaarborgd. Spearphishing-aanvallen zijn soms zo geraffineerd dat zelfs IT-beveiligingsexperts worden misleid. De legitimiteit van sommige phishing-berichten kan alleen goed worden bepaald na een uitvoerige technische analyse, maar de meeste medewerkers hebben daarvoor noch de tijd, noch de benodigde kennis. Om veiligheidslekken te voorkomen, zijn technologische maatregelen daarom de beste oplossing.

Zonder aandacht voor de oorzaken van de wachtwoord-problemen van uw medewerkers zult u geen succes hebben met uw pogingen uw instelling te beschermen tegen datalekken via social engineering.

Consolideer alle wachtwoorden van een medewerker in één veilig meesterwachtwoord

De hoofdoorzaken van veiligheidslekken door medewerkersfouten kunnen worden samengevat in drie punten:

- Medewerkers in de zorg hebben teveel wachtwoorden
- Ze moeten deze wachtwoorden te vaak invoeren
- En ze moeten bij het invoeren van al deze wachtwoorden teveel typen en klikken

Deze problemen nemen exponentieel toe in virtuele desktopinfrastructuren (VDI) met gedeelde werkstations, waarbij extra authenticatie en toegangsbeheer noodzakelijk is om roaming op meerdere apparaten mogelijk te maken. Zonder een oplossing voor de oorzaken van deze wachtwoordproblemen zijn uw inspanningen voor een waterdichte beveiliging van uw zorginstelling gedoemd te mislukken, evenals uw streven naar een optimaal rendement op uw investeringen in VDI.

De domeinwachtwoorden van uw medewerkers kunnen de toegangspoorten van uw netwerkperimeter wijd open zetten voor iedereen die zo'n wachtwoord in handen krijgt. U kunt deze toegangspoorten echter effectief vergrendelen en de meeste wachtwoorden overbodig maken door te kiezen voor een oplossing voor Single sign-on (SSO). Imprivata OneSign® Single Sign-On is de ideale tactische oplossing voor uw beveiligingsstrategie: wachtwoorden worden overbodig, omslachtige inlogprocedures behoren tot het verleden en – het belangrijkste – uw zorgverleners besparen veel tijd[13]. Een effectief systeem voor single sign-on biedt een doeltreffend antwoord op het riskante wachtwoordgedrag van uw medewerkers via een tweeledige verdedigingsstrategie:

- Het komt tegemoet aan het begrijpelijke verlangen van uw mensen naar tijdbesparing en gebruiksgemak

13. Imprivata OneSign bespaart klinische medewerkers aantoonbaar tot 45 minuten per dienst. Zie voor meer informatie het succesverhaal van het Mahaska Health Partnership: http://www.imprivata.com/sites/default/files/02-2014-Mahaska.pdf

In de zorg is het vrijwel onmogelijk wachtwoorden geheel overbodig te maken

- Het verhoogt de veiligheid zonder extra complexiteit voor de klinische workflows van uw medewerkers.

Er zijn in de zorg niet veel systemen die de beveiliging verbeteren én tegelijkertijd het gebruiksgemak vergroten, maar dit is precies wat u kunt bereiken met een effectieve SSO-oplossing. Het is een win-win-scenario voor uw beveiligingsstrategie.

Vergrendel de meesterwachtwoorden
Het is in de zorgsector vrijwel onmogelijk wachtwoorden geheel overbodig te maken, zelfs als u single sign-on aan uw beveiligingsarsenaal hebt toegevoegd. Veel essentiële klinische applicaties vereisen regelmatige invoer van wachtwoorden (vaak behoort dit tot de kernfunctionaliteit van EPD-software). Hier ligt de grote waarde van Imprivata OneSign Authenticatiebeheer: een systeem waarmee uw medewerkers automatisch sterke wachtwoorden kunnen invoeren met behulp van een badge of een vingerafdrukscan. Aan het begin van de dag loggen ze in met een wachtwoord of pincode. De rest van de dag hoeven ze alleen nog maar met hun badge te tikken of hun vingerafdruk te scannen om hun wachtwoorden in te vullen en toegang tot de klinische applicaties te krijgen.

Met een oplossing voor authenticatiebeheer gebruiken de medewerkers nog steeds een groot aantal wachtwoorden, maar hoeven ze deze niet meer allemaal te kennen, te onthouden of in te voeren. In feite bezitten ze nog steeds een hele verzameling wachtwoorden, maar ze kunnen deze niet verraden aan hackers, omdat ze er zelf geen toegang toe hebben.

In plaats daarvan gebruiken ze hun wachtwoorden op een indirecte en veilige manier. In tegenstelling tot een mens kan een goed ontworpen systeem voor authenticatiebeheer niet gemakkelijk worden misleid om geheime wachtwoorden prijs te geven. Een dergelijk systeem zal geen nagemaakte dialoogvensters invullen en het zal ook geen wachtwoorden delen of opslaan in niet-versleutelde bestanden. De medewerkerswachtwoorden en de patiëntendossiers worden veilig vergrendeld in een handig, bruikbaar systeem: een automatische technologie die niet gevoelig is voor misleiding en die nooit het slachtoffer zal worden van social engineering.

Informeer uw poortwachters
Nadat u de behoefte aan wachtwoorden sterk hebt verminderd met behulp van Imprivata OneSign Single Sign-On en Imprivata OneSign Authenticatiebeheer, kunt u een heel eenvoudige informatiestrategie volgen voor uw medewerkers.

Geef ze gewoon het goede nieuws: "Het zelf invoeren van wachtwoorden in applicaties is niet meer nodig, omdat de IT dit overbodig heeft gemaakt". Uw medewerkers weten voortaan dat er iets mis is als ze toch nog naar een applicatiewachtwoord worden gevraagd, zodat ze de IT-afdeling kunnen inlichten. Beter nog: u kunt uw systeem zodanig configureren dat uw medewerkers hun wachtwoorden niet meer zelf kúnnen intypen, omdat ze niet meer over deze informatie beschikken.

Voortaan hoeven ze alleen nog maar met hun badge te tikken of hun vingerafdruk te laten scannen.

Win de oorlog

De sleutel voor uw verdedigingsstrategie is gelegen in een helder inzicht in de unieke behoeften van uw organisatie, waardoor u het gedrag en de klinische workflows van uw mensen goed kunt observeren en beheren op een manier die ook hen voordelen oplevert.

Dit inzicht is cruciaal gebleken in de oorlog tegen cybercrime. U kunt deze strijd gemakkelijk in uw voordeel beslissen met de juiste technologie- en managementstrategieën. Door de behoeften en de zwakheden van uw menselijke perimeter actief te analyseren, wordt u een effectieve en succesvolle leider op het gebied van cyberbeveiliging. Want de beste leiders onderkennen altijd de zwakste plekken in hun verdedigingslinie en overzien het slagveld vanuit het eigen perspectief én vanuit het perspectief van de vijand.

Een strategisch partnerschap

Doorslaggevend bij het winnen van de vele veldslagen in de cyberbeveiliging is dat u beschikt over een waardevolle partner die verstand heeft van zorg en die uw behoeften begrijpt, die uw klinische workflows kent maar ook oog heeft voor de zwakke plekken hierin, en die uw organisatie helpt om ondanks deze zwakke plekken succesvol te opereren. Een SSO-oplossing is uw ideale partner: single sign-on ondersteunt de specifieke zwakke plekken van uw organisatie en transformeert ze tot sterke punten. Bezoek www.imprivata.com om te ontdekken waarom Imprivata de meest gevraagde SSO-leverancier is in de zorg.

Door de behoeften en de zwakheden van uw menselijke perimeter actief te analyseren, wordt u een effectieve en succesvolle leider op het gebied van cyberbeveiliging.

Imprivata

Imprivata is een toonaangevende leverancier van oplossingen voor authenticatie en toegangsbeheer in de zorgsector. De Imprivata-oplossingen voor single sign-on, authenticatiebeheer en beveiligde communicatie bieden snelle, veilige en efficiënte toegang tot IT-systemen in de gezondheidszorg, zodat vele beveiligingsproblemen worden opgelost en de zorgverleners productiever kunnen werken met meer aandacht voor de patiëntenzorg.

Meer dan 2 miljoen zorgverleners in ruim 1.000 zorginstellingen over de hele wereld vertrouwen op de oplossingen van Imprivata. Imprivata is de nummer 1 binnen de categorie SSO in de Best in KLAS Software & Services-rapporten over 2012 en 2013, en marktleider in de SSO-markt volgens HIMSS Analytics.

Voor meer informatie
kunt u bellen naar:
+1 781 674 2700
of bezoek ons online op:
www.imprivata.com

Kantoren in:
Lexington (MA), Verenigde Staten
Santa Cruz (CA), Verenigde Staten
Uxbridge, Groot-Brittannië
Parijs, Frankrijk
Nürnberg, Duitsland
Den Haag, Nederland

WP-EPCS-Ver1-0214