Onboarding:

Informationssäkerhetöverväganden

SECIFY

Innehållsförteckning

1. INFÖRANDET

Enbart tekniska åtgärder räcker inte för att skydda organisationens nätverks- och informationstillgångar när angripare utvecklar attackmetoder för att övervinna dessa åtgärder. Det är i slutändan den anställde som hanterar ett phishing-e-postmeddelande i sin brevlåda som kom igenom filtren som gör skillnaden. Därför är detavgörande för organisationer att förstå att deras anställda är den sista försvarslinjen när det gäller informationssäkerhet.

Som den sista försvarslinjen är det viktigt att medarbetaren är medveten om vikten av vaksamhet, krav och policys.

Den här guiden åtföljer videon för att ge vägledning till organisationen för att underlätta informationssäkerhet vid ombordstigning av personal till organisationen.

2. VAD SKA DE VETA?

2.1. FÖRORDNINGAR OCH ANDRA LAGKRAV

Anställda bör förstå att processer och policyer inte är utformade för att göra deras jobb svårare utan finns på plats för att följa lagkrav som lagstiftning eller avtalsförpliktelser för företaget.Det rekommenderas att arbetsbeskrivningar i organisationen hänvisar till efterlevnad av lagkrav, policyer och förfaranden så att personalen ser det som en integrerad del av sina jobb. Om personalen känner att säkerheten är en blockerare för deras arbete kommer de att bortse från säkerhetskraven eller hitta lösningar. Genom att integrera det i sin arbetsroll blir efterlevnad en del av "ett väl utfört jobb".

2.2. POLITIK

Ett av de största misstagen som organisationer gör är att försöka inkludera allt i en policy. Långa policyer är ofta olästa - personalen kommer att skumma igenom policyn och underteckna att de har läst den utan att faktiskt läsa den. Långa policyer kan också vara otydliga, vilket i kombination med skummad läsning leder till att personalen inte är tillräckligt medveten om de regler de måste följa.

Det rekommenderas att organisationer har tydliga politiska mål och inte försöker inkludera områden som kan stå ensamma som en policy. En informationssäkerhetsprincip kan till exempel referera till en IT-princip och en princip för mobila enheter för att hålla den kort. Mer detaljerad säkerhet för IT och mobila enheter kan ingå i den specifika policyn som täcker det ämnet.

En policy bör inte vara längre än 2 sidor. Om du inte har separata policyer att hänvisa till i den policy du skriver, kan specifik detaljerad information inkluderas i bilagor. Denna struktur gör det möjligt att vara kortfattad och tydlig i den mån den innehåller nödvändig information.

Policyer måste vara lätta att hitta så att personalen kan referera till dem när det behövs. Om personalen inte kan hitta en policy är det mer troligt att de ignorerar kraven.

2.3. INFORMATIONSHANTERING

Det är viktigt att anställda förstår vilken information de hanterar som en del av sitt jobb. Felaktig hantering av affärsinformation kan vara lika kostsamt för ett företag som felaktig hantering av personuppgifter.

Personalen bör förstå varför informationsklassificeringar ska användas och använda dem, särskilt för den mest känsliga informationen. Om data inte är märkta vet andra som informationen delas inte hur de ska hantera den.

En av de vanligaste källorna till överträdelser är omärkt information som av en annan anställd kan ses som inte känslig och därefter avslöjas utanför informationen.

Vid genomförandet av informationsklassificeringar bör regeln vara att endast genomföra de miniminivåer som är nödvändiga, helst högst 3. Ju fler nivåer du har, desto mer förvirring och avvikelser uppstår. Etiketter för extern, intern, känslig är till exempel lättare att förstå än det här exemplet från den brittiska regeringen som använde: Oklassificerad (extern), Oklassificerad men känslig (intern), Begränsad, Konfidentiell, Hemlig, Topphemlig.

I exemplet från den brittiska regeringen var resultatet av så många etiketter förvirring över vilka som gällde och människor hade olika tolkningar så att information av samma inverkan kunde märkas allt från oklassificerad extern till begränsad!

Det värsta resultatet av ett sådant system var att människor hamnade på den högsta klassificeringsnivån, vilket resulterade i att lunchinbjudningar klassificerades som begränsade. Ju mer information du har på högre klassificeringsnivåer, desto mer säkerhet behöver du och därför desto högre kostnad.

Helst bör säkerheten riktas för att skydda de mest känsliga tillgångarna - dagarna med att hålla inkräktare borta från nätverk är långt borta, så helst är den enda informationen som potentiellt kan äventyras extern information med låg påverkan. Klassificeringar och märkning hjälper organisationen att prioritera säkerhetsåtgärder för att minimera säkerhetsöverträdelser. Resultatet är lägre kostnad för säkerhetsåtgärder, lägre kostnad när ett intrång inträffar och mindre skada och påverkan på rykte i sådana situationer.

2.4. INFORMATIONSHANTERING: DELA INFORMATION

E-post är den främsta orsaken till överträdelser med information som avslöjas för fel person eller skickas osäker. Anställda måste göras medvetna om hur de ska dela data externt om det behövs utan att skicka data via e-post.

Helst bör organisationen titta på att ge begränsad åtkomst till externa resurser för att komma åt informationen, till exempel att tillåta externa betrodda gäster till Teams så att informationen inte behöver lämna organisationen.

Om detta inte är möjligt och information måste avslöjas externt och e-post är det enda alternativet, bör känslig affärsinformation och personuppgifter krypteras. Underlåtenhet att kryptera personuppgifter som skickas okrypterade kommer sannolikt att öppna organisationen för böter.

En organisation bör titta på hur man bäst implementerar dessa åtgärder och se till att eventuella dekrypteringsnycklar delas säkert med mottagaren. IT-resurser i en organisation ska kunna hjälpa till och underlätta säker kommunikation.

2.5. DOKUMENTATION

Hållbarhetsåtgärder för att minska utskrifter har påverkat informationssäkerheten eftersom det med färre dokument som skrivs ut finns en minskad risk för förlorade dokument. Helst bör personalen uppmuntras att inte skriva ut dokument så långt det är möjligt för att minska risken för att dokumentet går förlorat.

Om dokument skrivs ut bör organisationen ha en tydlig policy för hur de ska hanteras – som att inte lämna dem obevakade på skrivbord för obehörig visning, att inte tillåta att de mest känsliga dokumenten tas hem och se till att det finns en säker avfallshanteringspolicy som att strimla känsliga dokument.

Dokumentförstörare bör göras tillgängliga – dessa bör vara tvärskurna dokumentförstörare. Om en dokumentförstörare inte är tvärskuren skulle en extremt bestämd hackare kunna rekonstruera dokumenten.

3. SLUTSATS

Det finns ett antal åtgärder som organisationen kan vidta för att säkerställa att anställda är medvetna om informationssäkerhetsaspekterna av sina handlingar och för att informera dem om varför de är skyldiga att följa specifika processer.

Den mest kritiska delen av dessa åtgärder är att se till att personalen vet vem de ska rapportera en incident till och kan göra det enkelt och snabbt. Underlåtenhet att säkerställa rapportering av informationssäkerhetsöverträdelser görs snabbt kan vara betydande.

<