Onboarding:

Cybersäkerhetöverväganden

SECIFY

Innehållsförteckning

1. INFÖRANDET

Den här guiden följer med videon för att ge råd till organisationen hur man underlättar cybersäkerhetsförståelse med sina anställda.

Det är viktigt att alla som arbetar i en organisation förstår att säkerhet är allas ansvar. Säkerhet är inte bara uppdraget för informationssäkerhetsansvariga eller CISO: er.

Effekterna av säkerhetsöverträdelser kan vara betydande - bortsett från de potentiella böterna på 4% av den globala omsättningen för GDPR-överträdelser, har större säkerhetsincidenter i vissa fall resulterat i konkurs eller nedskärningar eller organisationen.

Till exempel förlorade Talk Talk 2015 över 100 000 kunder efter 3 allvarliga (och undvikbara) överträdelser som resulterade i identitetsstöld för några av deras kunder. Det tog Talk Talk över 3 år att få tillbaka sin omsättning till 2015 års nivå och uppnåddes endast genom att i huvudsak tillhandahålla ultralåga tjänster för att vinna tillbaka kunder.

Det är viktigt att all personal förstår att angripare kommer att rikta in sig på dem oavsett deras position i företaget för att få tillgång till företagets nätverk.

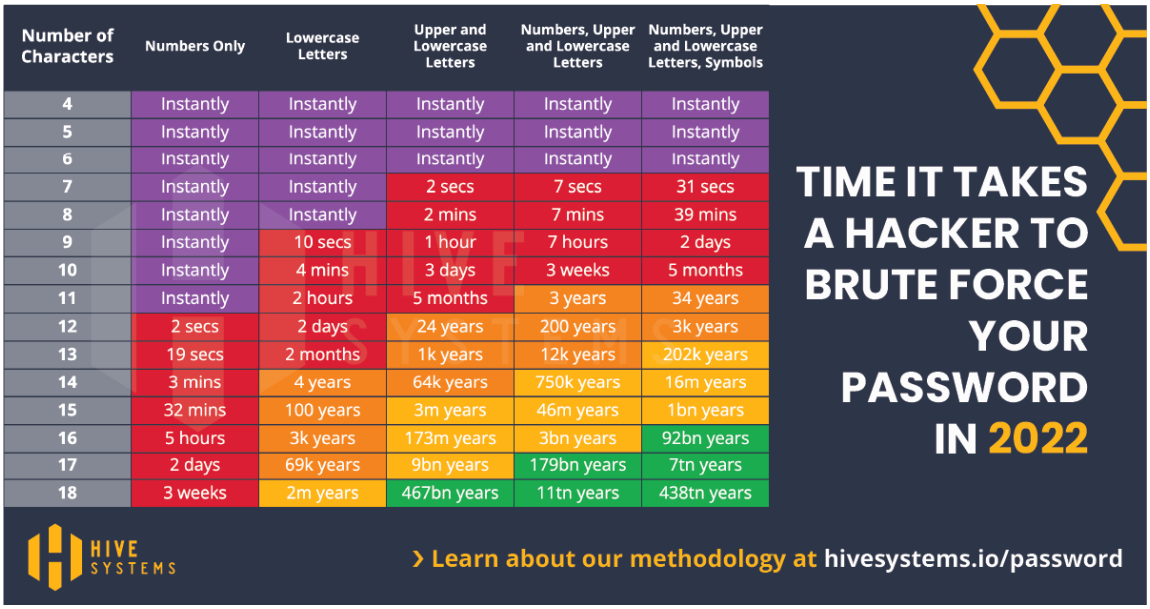
Det är ofta en bra idé att förmedla till personalen att grundläggande cybersäkerhetsåtgärder som krävs av verksamheten också är god praxis för att skydda deras personuppgifter i deras system hemma.

2. VAD SKA DE VETA?

2.1. LÖSENORD

Det bör förmedlas till anställda att de inte ska använda lösenord som de använder för personliga konton för sina arbetskonton. Kompromitterade lösenord säljs ofta på Dark Web och angripare kommer att använda dem mot en persons arbetskonton.

Helst bör en lösenfras användas istället för ett lösenord. En lösenfras gör det lättare att komma ihåg längre lösenord – följande tabell visar den aktuella beräknade tiden för att bryta lösenord baserat på längd och komplexitet:



Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

I grund och botten, ju längre och mer komplex lösenfrasen är, desto säkrare är lösenordet.

Lösenordspolicyer bör vara mycket tydliga när det gäller krav på längd och komplexitet samt historikpolicyer för återanvändning av lösenord. Detta bör också innehålla instruktioner om att inte använda personlig information, till exempel barns namn eller födelsedatum, för att basera lösenordet / lösenfrasen på - socialteknik är en vanlig metod som används av angripare för att gissa lösenord som används av människor.

Policyer bör också tillämpa kravet på att aldrig dela lösenord inom organisationen. Arbetsprocesser bör upprättas för att undvika att den situationen blir nödvändig. Organisationen bör också ha en policy för åtkomst till en annan användares data, till exempel om den användaren går på långtidssjukskrivning, för att säkerställa att lösenord inte delas. Delning av lösenord är inte bara en säkerhetsrisk utan tar också bort allt ansvar i händelse av ett intrång.

2.2. MFA

Multifaktorautentisering (MFA) bör implementeras på system för att lägga till ytterligare en säkerhetsnivå. MFA använder två (tvåfaktorsautentisering eller 2FA) eller flera av dessa faktorer:

- Något du vet (t.ex. lösenord)
- Något du har (t.ex. mobiltelefon)
- Något du är (t.ex. biometri)

När du använder 2FA med en mobiltelefon rekommenderas att personalen använder autentiseringsappar snarare än att förlita sig på SMS-texter. SMS-texter är inte säkra och kan fångas upp så autentiseringsappar ger en säkrare 2FA.

2.3. NÄTFISKE

Phishing är en vanlig attackmetod av hackare på organisationer. Även om de flesta har tekniska åtgärder för att minska risken är det viktigt att personalen ofta påminns om risken.

Personalen bör vara medveten om att nätfiske är utformat för att psykologiskt manipulera människor till att reagera på ett e-postmeddelande - detta är en anledning till att sådana e-postmeddelanden ofta har en brådskande karaktär för dem. En annan psykologisk manipulation är att utnyttja vår rädsla för att missa - att erbjuda något som mottagaren kanske vill ha som kanske inte är tillgängligt länge är en annan typisk attackmetod.

Som en del av phishing-utbildningen bör personalen rådas att följa STAR-metoden. STAR definierar:

- **Stopp**
- **Think**
- **Ask**
- **Respond**

Organisationen måste se till att personalen enkelt kan rapportera phishing-e-postmeddelanden - det finns ofta en phishing-knapp som kan användas i e-postklienter för att personalen ska kunna göra detta enkelt. Personalen ska känna att de kan rapportera allt misstänkt fritt snarare än att inte använda det här verktyget.

En viktig del av all phishing-utbildning är att utbilda personalen att inte bara vara försiktig med externa oväntade e-postmeddelanden utan också interna. Om ett konto komprometteras skickar angripare ofta ut interna e-postmeddelanden för att kompromettera andra interna konton.

Om en länk eller ett e-postmeddelande är oväntat och inte ingår i den normala arbetsrutinen, bör anställda validera med personen i organisationen via telefon för att bekräfta att det är ett legitimt e-postmeddelande. Organisationer bör ha mekanismer på plats på alla Microsoft-plattformar för att säkerställa att alla komprometterade konton som används på detta sätt tar bort alla internt skickade phishing-e-postmeddelanden som en prioritet.

2.4. ENHETER

Organisationer står inför en rad utmaningar när det gäller huruvida de ska använda officiella enheter eller låta personalen komma åt företagsresurser från personliga enheter.

Policyn beror på organisationens riskaptit och ekonomiska överväganden, men ur ett säkerhets- och integritetsperspektiv bör officiella enheter användas så långt som möjligt. Om en organisation tillåter användning av personliga enheter bör den se till att det finns en tydlig åtskillnad mellan affärsdata och personuppgifter på enheten med hjälp av en MDM (Mobile Device Manager). Detta bör testas för att säkerställa att det i händelse av att behöva rensa affärsdata inte kommer att torka den anställdes hela telefon. GDPR-reglerna kräver också att MDM inte får kunna komma åt den anställdes personuppgifter.

Vid användning av officiella produkter bör tekniska åtgärder införas för att förhindra obehörig nedladdning av programvara. Detta minskar risken för att införa skadlig kod och virus på enheten, men säkerställer också att organisationen inte får licensproblem i framtiden.
Alla enheter, både personliga och företag, ska krypteras och skyddas med adekvat MFA. Detta säkerställer att risken för intrång minimeras om enheter går förlorade.

Säkerhetsprogramvara på enheten bör också installeras så att enhetens plats och fjärradering kan utföras om enheten går förlorad eller blir stulen.

2.5. DISTANSARBETE

Organisationer som tillåter distansarbete bör ha en tydlig policy för hur detta ska följas för att säkerställa att sekretess- och säkerhetskraven uppfylls.

Dessa åtgärder bör omfatta tillhandahållande av en VPN för att säkerställa säker kommunikation, sekretessskärmar för bärbara datorer om personal arbetar med kollektivtrafik och ett krav på att inte behålla säkerhetsinformation eller tokens med enheten.

Personalen bör rådas att vara mycket försiktig med att ansluta till offentliga WiFi-nätverk där kommunikation och referenser kan fångas upp och äventyras. De bör rådas att ägna särskild uppmärksamhet åt WiFi-nätverksnamn, till exempel kunna skilja mellan exempelvis Mariott och Mari0tt.

3. SLUTSATS

Organisationer som förklarar cybersäkerhetsåtgärder för anställda och att alla har en viktig roll i att skydda verksamheten kommer att minimera sina risker för cybersäkerhetsincidenter. Det är absolut nödvändigt att se till att alla anställda är informerade, förstår kraven och var man kan hitta information eller vem man ska kontakta även om frågor eller en incident.
Personalen bör förstå effekterna av att kringgå säkerhetsåtgärder eller hitta lösningar och att det kan leda till ett betydande intrång.