Vážený pane, vážená paní,

dovolte mi Vás touto cestou informovat o významném nárůstu níže uvedených rizik v souvislosti s nemocí Covid-19.

KYBERNETICKÁ RIZIKA

Přesouváte větší či menší část svých zaměstnanců na **Home Office?** V souvislosti s náhlou nutností práce za využití vzdáleného přístupu: **Remote Desktop Protocol – RDP** stoupá (nejen) riziko kybernetického útoku! Existují čtyři hlavní témata, které je dobré mít na paměti během přizpůsobení se novému provoznímu režimu. Tato témata uvádíme níže, nicméně **naším doporučením je zvážit zavedení pojistné ochrany proti kybernetickým rizikům** obzvláště, bude-li fungování Vaší společnosti na vzdáleném přístupu do větší míry záviset.

1) RIZIKO SPOJENÉ SE VZDÁLENÝM PŘÍSTUPEM

Podle údajů londýnské pojišťovny CFC Underwriting bylo **80% všech pojistných událostí souvisejících s narušením bezpečnosti systémů způsobeno slabinami v RDP**. I přes nasazení vícefaktorového přihlašování jde nadále o nejzranitelnější část Vaší kybernetické integrity. Další nebezpečí mohou představovat přetížení serverů a následný výpadek. Ujistěte se, že Vaše vzdálená síť je adekvátně zabezpečená a servery zajišťující vzdálený přístup, které využíváte mají dostatečnou kapacitu.

2) NOVÁ PŘÍLEŽITOST K PHISHINGU

Pojem phishing je dnes již známým názvem pro **podvodné emaily** svádějící ke kliknutí na odkaz či stažení přílohy. Hackeři mají nyní šanci využít chaosu kolem Coronaviru k tvorbě emailů tvářících se jako firemní zpráva pro zaměstnance, informace od státu popř. od dalších poplatných činitelů. Napomáhá jim i všeobecný shon a urgentnost nastalé situace.

3) NEDOSTATEK ODBORNÝCH KAPACIT

Fungování Vaší sítě může záviset na větším či menším počtu dodavatelů. Možná využíváte cloudy. Nebo Vám systémy spravuje dodavatelská společnost. V nastalé situaci lze očekávat **prodlouženou reakční dobu** těchto odborných společností a jednotlivců v případě komplikací, technických problémů či kybernetických incidentů. Prověřte své interní pracovníky i IT dodavatele, zdali jsou na nastalou situaci připraveni!

4) POTŘEBNÝ HARDWARE

Mnoho společností současně čelí potřebě nákupu notebooků a jiných mobilních zařízení pro práci z domova. Jedno ze základních pravidel kybernetické bezpečnosti je volba jednotného dodavatele vybavení. Jelikož současná nabídka hardware je kriticky omezená (velká část elektroniky a počítačů se vyrábí v Číně), stojí mnoho společností před volbou, zda nemít dostatek notebooků pro všechny zaměstnance, kteří mají pracovat vzdáleně, či zda vpustit do společnosti **hardware od nového výrobce, což může kompromitovat bezpečnost Vašich systémů**.

Josef Majer, Senior Client Executive
MARSH, s.r.o. | Financial and Professional Lines
Atrium Flora, vchod B, Vinohradská 2828/151, 130 00 Praha 3 – Vinohrady
josef.majer@marsh.com
+420 221 418 164 | +420 730 573 931
www.marsh.cz

LEADERSHIP, KNOWLEDGE, SOLUTIONS...WORLDWIDE.