**Kontakt dla mediów:**

Patrycja Kaleta-Łuczynowicz

[patrycja.kaleta@linkleaders.pl](mailto:patrycja.kaleta@linkleaders.pl)

+48 505 223 994

Olga Skarżyńska

[olga.skarzynska@linkleaders.pl](mailto:olga.skarzynska@linkleaders.pl)

+48 510 382 420

**Pacjenci i lekarze na celowniku cyberprzestępców**

**– Ochrona zdrowia jest jednym z najczęściej atakowanych przez cyberprzestępców sektorów – przestrzegają specjaliści ds. cyberbezpieczeństwa ESET. Wyciek danych osobowych pacjentów, szczegółów dotyczących schorzeń i metod leczenia to poważne zagrożenie. Cyberprzestępcy organizują także ataki paraliżujące całe instytucje ochrony zdrowia.**

Ostatnio głośno było m.in. o wycieku danych osobowych, jakiego doświadczył jeden z amerykańskich dostawców urządzeń medycznych. Firma, dostarczająca pacjentom z wysokim ryzykiem nagłej śmierci sercowej przenośne defibrylatory, przyznała, że została zaatakowana przez cyberprzestępców. W ramach incydentu mogły zostać wykradzione dane nawet miliona jej byłych i obecnych klientów. W podobnym czasie inni cyberprzestępcy wzięli na cel system komputerowy jednego ze szpitali w Barcelonie, poważnie utrudniając jego funkcjonowanie i pozbawiając lekarzy m.in. dostępu do aktualnych danych na temat pacjentów. Z kolei w Polce m.in. na początku lutego br. miał miejsce atak na Centralny Szpital Kliniczny w Łodzi. Instytucja poinformowała, że doprowadził on do czasowego, profilaktycznego wyłączenia systemów informatycznych.

– Wśród konsekwencji potencjalnych ataków na służbę zdrowia należy wymienić operacyjny paraliż instytucji, wyłudzenia tożsamości pacjentów, wymuszenia środków pieniężnych, a nawet zakłócenia i ingerencje w procedury medyczne (w przypadku, jeśli złośliwym oprogramowaniem zostaną zainfekowane urządzenia medyczne). Dane osobowe i dotyczące zdrowia, to potężna karta przetargowa dla cyberprzestępców. W sektorze zdrowia przetwarza się bardzo duże wolumeny takich informacji, a więc i ryzyko jest spore. Wizje zakładające, że niepowołane osoby uzyskają dostęp do nieprawidłowo zabezpieczonych urządzeń medycznych i będą chciały zaingerować w zdrowie i życie pacjentów to dość apokaliptyczne scenariusze, ale trudno przypisywać cyberprzestępcom jakiekolwiek etyczne motywacje w momencie, gdy dostrzegą możliwość działania – komentuje **Kamil Sadkowski, starszy specjalista ds. cyberbezpieczeństwa ESET.**

Jak podkreślają eksperci ds. cyberbezpieczeństwa, ryzyko ataków na infrastrukturę krytyczną w wielu różnych krajach wzrosło także od czasu agresji Rosji na Ukrainę, a instytucje zajmujące się ochroną zdrowia znajdują się wśród najczęściej namierzanych przez cyberprzestępców.

Cyberataki to oczywiście także nieodłączny koszt związany z transformacją cyfrową każdego sektora. W placówkach medycznych coraz częściej wdrażane są e-usługi, a nowoczesny sprzęt medyczny jest połączony z internetem, m.in. w celu transmisji i przetwarzania danych medycznych pacjentów. Cyfryzacji powinna jednak towarzyszyć równoległa troska o nowoczesne zabezpieczenia, a także szkolenie personelu.

– Sektor zdrowia jest jedną z najczęściej atakowanych przez cyberprzestępców branż, często organizują oni także ataki przy użyciu złośliwego oprogramowania, wymierzone w organizacje zajmujące się zdrowiem i życiem ludzi. To bardzo niepokojące. Widzimy również wyraźnie, że tego typu akcje bywają powtarzalne. Zdarza się, że atakujący wracają do swoich wcześniejszych celów, podejmując kolejne próby szkodliwych działań i licząc na to, że nie zostały wdrożone żadne środki zapobiegawcze. Branża medyczna musi mieć świadomość, jak ważna jest ochrona danych i jaki wpływ na organizacje i pacjentów mogą mieć ewentualne zaniedbania w tej kwestii – przestrzega **Kamil Sadkowski, starszy specjalista ds. cyberbezpieczeństwa ESET.**